NIST Special Publication 800-60
Version 1.0

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

William C. Barker

I N F O R M A T I O N S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

December 2003

U.S. DEPARTMENT OF COMMERCE
Donald L. Evans, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary of Commerce for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Arden L. Bement, Jr., Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national security-related information in Federal information systems. This special publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

The National Institute of Standards and Technology (NIST) has developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

National Institute of Standards and Technology, Draft Special Publication 800-60 Natl. Inst. Stand. Technol. Spec. Publ. 800-60, Volume II, 266 pages (*December 2003*)

THE PUBLIC COMMENT PERIOD FOR THIS DOCUMENT BEGINS ON 19 DECEMBER, 2003 AND ENDS ON 20 FEBRUARY 2004. COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, NIST, VIA ELECTRONIC MAIL AT 800-60_COMMENTS@NIST.GOV

OR VIA REGULAR MAIL AT

100 BUREAU DRIVE (MAIL STOP 8930)
GAITHERSBURG, MD 20899-8930

Acknowledgements

The author wishes to thank his colleagues who reviewed drafts of this document and contributed to its development. The authors also gratefully acknowledge and appreciate the many comments from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Note to Reviewers

This is Volume II of two volumes. It contains the appendices to NIST Special Publication 800-60.

NIST Special Publication 800-60 may be used by organizations in conjunction with an emerging family of security-related publications including:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (Pre-publication final), December 2003;
- NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (Second public draft), June 2003;
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, (Initial public draft), October 2003.
- NIST Special Publication 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems* (Initial public draft), Spring 2004;
- NIST Special Publication 800-59, *Guide for Identifying an Information System as a National Security System*, August 2003; and
- FIPS Publication 200, *Minimum Security Controls for Federal Information Systems*, (Projected for publication, Fall 2005)[1]

The series of seven documents, when completed, is intended to provide a structured, yet flexible framework for selecting, specifying, employing, and evaluating the security controls in Federal information systems—and thus, make a significant contribution toward satisfying the requirements of the Federal Information Security Management Act (FISMA) of 2002. We regret that all seven publications could not be released simultaneously. However, due to the current international climate and high priority of information security for the Federal government, we have decided to release the individual publications as they are completed. While the publications are mutually reinforcing and have some dependencies, in most cases, they can be effectively used independently of one another.

It should be noted that this initial draft of Special Publication 800-60 is preliminary in nature. The information types and security impact levels are based on the OMB Federal Enterprise Architecture Program Management Office *Business Reference Model 2.0* and FIPS 199, respectively. Rationale for initial impact level recommendations have been incorporated from multiple sources, and as such, will require several iterations of review, comment, and subsequent modification to achieve consistency in terminology, structure, and content. The prerequisite role played by security categorization in selection of SP 800-53 security controls, and the importance of security controls in the protection of Federal information systems demands early exposure to the community who will be employing those controls and thus, motivated the release of this document as the earliest opportunity.

Reviewers are encouraged to provide comments on any aspect of this special publication. Of particular interest are comments on: (i) the level of granularity established for information types; (ii) the information type selection and organization; (iii) the impact levels recommended for each information type; (iv) the rationale provided for security categorization recommendations; (v) the assumptions underlying common integrity and availability impact level decisions as reflected in the rationale; and (vi) understandability and usability of the guideline.

Your feedback during the public comment period is essential to the document development process and is greatly appreciated.

[1] FIPS Publication 200, *Minimum Security Controls for Federal Information Systems*, when published in 2005, will replace NIST Special Publication 800-53 and become a mandatory standard for Federal agencies in accordance with the Federal Information Security Management Act (FISMA) of 2002.

[This Page Intentionally Left Blank]

EXECUTIVE SUMMARY

Title III of the E-Government Act (Public Law 107-347), titled the Federal Information Security Management Act (FISMA), tasked the National Institute of Standards and Technology (NIST) to develop:

- Standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each such category; and
- Minimum information security requirements (i.e., management, operational, and technical controls), for information and information systems in each such category.

In response to the second of these tasks, this guideline has been developed to assist Federal government agencies to categorize information and information systems. The guideline's objective is to facilitate provision of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or loss of availability of the information or information system. This guideline assumes that the user has read and is familiar with *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199). The guideline:

- Reviews the security categorization terms and definitions established by FIPS 199;
- Recommends a security categorization process;
- Describes a methodology for identifying types of Federal information and information systems;
- Suggests provisional or default security impact levels for common information types;
- Discusses information attributes that may result in variances from the basic impact level assignment; and
- Describes how to establish a system security categorization based on the system's use, connectivity, and aggregate information content.

Types of information can normally be divided into 1) that information associated with an agency's mission-specific activities and 2) that information associated with administrative, management, and support activities common to most agencies. In this guideline, administrative, management, and support information is referred to as *agency-common* information. Security attributes of information associated with mission-specific activities will often vary from agency to agency. Consequently, for purposes of this guideline, the mission-specific information will be termed *agency-specific*. This

guideline addresses agency-specific information separately from agency-common information. Because of the degree to which consequences of security compromise of agency-specific information vary among different operational environments, this guideline is less prescriptive in the case of agency-specific information than in the case of agency-common information. Similarly, the specialized knowledge of information types, information use, and program and mission life-cycle context on which the sensitivity of agency-specific information is dependent is concentrated within the agency responsible for that mission information. While specific agency-common information types are discussed in detail in this document, the treatment of agency-specific information is limited to general guidelines for identification of information types and assignment of impact levels. (Examples of agency-specific information types are discussed in Appendix D).

This document is intended as a reference resource rather than as a tutorial. Not all of the material will be relevant to all agencies. This document includes two volumes, a basic guideline and a volume of appendices. Users should review the guidelines provided in Volume I, then refer to only that specific material from the appendices that applies to their own systems and applications.

The basis employed in this guideline for the identification of information types is the Office of Management and Budget's Federal Enterprise Architecture Program Management Office June 2003 publication, *The Business Reference Model Version 2.0* (*BRM*). The *BRM* describes functions relating to the purpose of government (missions, or *services to citizens*), the mechanisms the government uses to achieve its purpose (*modes of delivery*), the support functions necessary to conduct government (*support services*), and the resource management functions that support all areas of the government's business (*management of resources*). The information types associated with *support services* and *management of resources* functions are treated as agency-common types. Default confidentiality, integrity, and availability information categories are recommended for each agency-common information type. Rationale underlying the recommended default impact levels is provided in Appendix C. The information types associated with *services to citizens* and *modes of delivery* functions are treated as agency-specific. Recommended default information security categories, underlying rationale, and examples of bases for deviation from the recommended defaults for agency-specific information types are provided in Appendix D.

Some information has been established in law, by Executive Order, or by agency regulation as requiring protection from disclosure. Appendix E addresses legal and executive sources that establish sensitivity and/or criticality characteristics for information processed by Federal government departments and agencies. Individual citations from the United States Code are listed in the appendix.

GUIDE FOR MAPPING TYPES OF INFORMATION AND INFORMATION SYSTEMS TO SECURITY CATEGORIES

Volume II: Appendices

Table of Contents

[This Page Intentionally Left Blank]

APPENDIX A: GLOSSARY OF TERMS

Agency - The term 'agency' means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the government (including the Executive Office of the President), or any independent regulatory agency, but does not include -

(a) the General Accounting Office;
(b) Federal Election Commission;
(c) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or
(d) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.

Authentication - Security control designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Authenticity - The property of being genuine and able to be verified and be trusted. See authentication.

Availability - The term 'availability' means ensuring timely and reliable access to and use of information.

Classified Information –
Classified information or classified national security information means information that has been determined pursuant to E.O. 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Command and Control –
'Command and Control' is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Confidentiality - The term 'confidentiality' means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Counterintelligence – The term 'counterintelligence' means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

Criticality - The term 'criticality' refers to the incorrect behavior of a system. The more serious the expected direct and indirect effects of incorrect behavior, the higher the criticality level.

Cryptologic - The term 'cryptologic' means of or pertaining to cryptology.

Cryptology - 'Cryptology' is the science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence.

Executive Agency - An 'executive agency' is an executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec.102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); or a wholly owned government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

Federal Information System – A 'Federal information system' is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

Impact - The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Independent Regulatory Agency – The term 'independent regulatory agency' means the Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Energy Regulatory Commission, the Federal Housing Finance Board, the Federal

Maritime Commission, the Federal Trade Commission, the Interstate Commerce Commission, the Mine Enforcement Safety and Health Review Commission, the National Labor Relations Board, the Nuclear Regulatory Commission, the Occupational Safety and Health Review Commission, the Postal Rate Commission, the Securities and Exchange Commission, and any other similar agency designated by statute as a Federal independent regulatory agency or commission.

Individual - The term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence. Agencies may, consistent with individual practice, choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.

Information Resources –
The term 'information resources' means information and related resources, such as personnel, equipment, funds, and information technology.

Information Security -
The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

Information System - The term 'information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information Technology –
The term 'information technology', with respect to an executive agency means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information

technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Integrity - The term 'integrity' means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Intelligence - The term 'intelligence' means (1) the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; or (2) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The term 'intelligence' includes foreign intelligence and counterintelligence.

Intelligence Activities –

The term 'intelligence activities' includes all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333, United States Intelligence Activities.

Intelligence Community –

The term 'intelligence community' refers to the following agencies or organizations:
(1) The Central Intelligence Agency (CIA);
(2) The National Security Agency (NSA);
(3) The Defense Intelligence Agency (DIA);
(4) The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
(5) The Bureau of Intelligence and Research of the Department of State;
(6) The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy; and
(7) The staff elements of the Director of Central Intelligence.

National Security System –

A 'national security system' is any information system (including any telecommunications system) used or operated by an agency or by a contractor on behalf of an agency, or any other organization on behalf of an agency – (i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapon system; or is critical to the direct

fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Non-repudiation - Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later legitimately deny having processed, stored, or transmitted the information.

Privacy Impact Assessment (PIA) –
A 'Privacy Impact Assessment' is an OMB-mandated analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Public Information - The term 'public information' means any information, regardless of form or format that an agency discloses, disseminates, or makes available to the public.

Risk - As used in this guideline, the term 'risk' means a combination of: (i) the likelihood that a particular vulnerability in an agency information system will be either intentionally or unintentionally exploited by a particular threat resulting in a loss of confidentiality, integrity, or availability, and (ii) the potential impact or magnitude of harm that a loss of confidentiality, integrity, or availability will have on agency operations (including mission, functions, and public confidence in the agency), an agency's assets, or individuals (including privacy) should there be a threat exploitation of information system vulnerabilities.

Security Category - The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on an agency's assets or operations (including mission, functions, and public confidence in the agency).

Security Controls - 'Security controls' are the management, operational, and technical controls (safeguards or countermeasures) prescribed for an information system which, taken together, satisfy the system's

specified security requirements and adequately protect the confidentiality, integrity, and availability of the system and its information.

Security Objectives - Confidentiality, integrity, and availability.

Sensitivity - The term 'sensitivity' is used in this guideline to mean a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

Telecommunications –
The term 'telecommunications' means the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

Threat - A 'threat' is any circumstance or event with the potential to intentionally or unintentionally exploit a specific vulnerability in an information system resulting in a loss of confidentiality, integrity, or availability.

Vulnerability - A 'vulnerability' is a flaw or weakness in the design or implementation of an information system (including security procedures and security controls associated with the system) that could be intentionally or unintentionally exploited to adversely affect an agency's operations (including missions, functions, and public confidence in the agency), an agency's assets, or individuals (including privacy) through a loss of confidentiality, integrity, or availability.

Weapons System - A 'weapons system' is a combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.

APPENDIX B: References

Business Reference Model 2.0, Federal Enterprise Architecture Program Management Office, Office of Management and Budget, June 2003.

E-Government Act of 2002, Public Law 107-347, December 17, 2002.

Federal Information Security Management Act of 2002, Public Law 107-347, Title III, December 17, 2002.

Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems, NIST Special Publication 800-37 (SP 800-37), Version 1.0, National Institute of Standards and Technology, October 2002.

Information Technology Management Reform Act of 1996, Public Law 104-106, August 1996.

"OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," Office of Management and Budget Memorandum, Office of Management and Budget, September 29, 2003.

Paperwork Reduction Act of 1995, Public Law 104-13, May 1995.

Privacy Act, Public Law 93-579, (5 U.S.C. § 552A), December 1974 (effective September 27, 1975).

Protecting America's Critical Infrastructures, Presidential Decision Directive 63, Executive Office of the President, May 22, 1998.

Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53 (SP 800-53), Version 1.9, National Institute of Standards and Technology, October 2003.

Security of Federal Automated Information Resources, OMB Circular No. A-130, Appendix III, February 1996.

Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publication 199 (FIPS 199), Version 2.0, National Institute of Standards and Technology, December 2003

USA Patriot Act, Public Law 107-56, Titles VII and Title IX, October 26, 2001.

[This page intentionally left blank.]

APPENDIX C: RATIONALE FOR AGENCY-COMMON INFORMATION AND INFORMATION SYSTEMS IMPACT LEVELS

Much Federal government information and many systems are not employed directly to provide services to citizens, but are primarily intended to provide administrative or business services that support mission accomplishment. Section 4, "Impact Levels by Type for Agency-Common Information," suggests a set of information types for agency-common information and recommended default security categories. As stated in Section 4, the basis employed in this guideline for the identification of information types is the Office of Management and Budget's Federal Enterprise Architecture Program Management Office June 2003 publication, *The Business Reference Model Version 2.0* (*BRM*).

Most information systems employed in both direct service and administrative/ management support activities perform one or more of the service delivery support functions described in Appendix C.1, "Services Delivery Support Information." These service support functions are the day-to-day activities necessary to the organizations that provide services to the general population and administrative/management services to government departments and agencies responsible for the provision of those services. As in the case of administrative/business information and information systems, the security objectives and impacts are determined by the direct service missions and constituencies ultimately being supported. It is likely that all Federal government information systems store, process, and operate under the control of information technology (IT) infrastructure maintenance information (e.g., password files and file and network access settings). At least a basic set of security controls will apply to this set of information and processes in order to combat potential corruption, misuse, or abuse of system information and processes.

Information necessary to conduct administrative or business services that support mission accomplishment includes the government resource management information types described in Appendix C.2, "Government Resource Management Activities." All of the departments and agencies performing direct service functions are supported by information systems that perform the activities described in Appendix C.2. Many departments and agencies operate their own support systems. Others obtain at least some support services from other organizations. Some agencies' missions are primarily to support other government departments and agencies in the conduct of direct service missions. As indicated above, security objectives and impacts for administrative and management information and systems are determined by the natures of the supported direct services and constituencies being supported.

Note that much of the discussion of factors affecting assignment of impact level is common to many information types. Because this guideline is intended as a reference document, and it is anticipated that most users will refer only to one or a few information types of interest, several common or similar observations appear with each information type to which they are appropriate. Some impact factors common to all information types are discussed in Section 3.3.

C.1 Services Delivery Support Information

Services delivery support functions provide the critical policy, programmatic, and managerial foundation to support Federal government operations. Security objectives and impact levels for service delivery support information and systems are generally determined by the natures of the supported direct services and constituencies being supported. Note that if a system stores, processes, or communicates *national security* information, it is defined as a *national security system*, and is outside the scope of this guideline.[2] Service delivery support activities are defined below:

C.1.1 Controls and Oversight

Controls and Oversight information is used to ensure that the operations and programs of the Federal government and its external business partners comply with applicable laws and regulations and prevent waste, fraud, and abuse.

C.1.1.1 Corrective Action Information Type

Corrective Action involves the enforcement functions necessary to remedy programs that have been found non-compliant with a given law, regulation, or policy. The recommended security categorization for the corrective action information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1.1.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of corrective action information on the ability of responsible agencies to remedy internal or external programs that have been found non-compliant with a given law, regulation, or policy. Unauthorized disclosure of most corrective action information should have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974 or information that is proprietary to a corporation or other organization. Such information will often be assigned a ***moderate*** confidentiality impact level.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for the corrective action information type is ***low***.

[2] A *national security system* is any information system (including any telecommunications system) used or operated by an agency or by a contractor on behalf of an agency, or any other organization on behalf of an agency – (i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions (excluding a routine administrative or business applications system used for applications such as payroll, finance, logistics, and personnel management); or (ii) that processes classified information.

C.1.1.1.2 Integrity

The consequences of undetected unauthorized modification or destruction of corrective action information can conceivably compromise the effectiveness of compliance enforcement actions (e.g., by providing violators with a basis for claiming investigative or enforcement irregularities, thus supporting legal challenges to proposed corrective actions).

Special Factors Affecting Integrity Impact Determination: Where the damage likely to be caused by unauthorized modification or destruction of corrective action information is detected and corrected before it adversely affects agency operations or public confidence in the agency, the base integrity impact level assigned to corrective action information can be ***low***. The consequences of unauthorized modification of corrective action information that is not time-critical can typically be addressed by basic procedures and controls. Little, if any, corrective action information is acted on in real time. Consequently, the information is relatively unlikely to be acted on before the modification or destruction on information is detected.

Recommended Integrity Impact Level: In general, the default integrity impact level recommended for corrective action information is ***low***.

C.1.1.1.3 Availability

The effects of disruption of access to or use of corrective action information can usually be repaired. The availability impact is dependent on the time frame required for repair.

Special Factors Affecting Availability Impact Determination: Corrective action processes are generally tolerant of reasonable delays, and the consequences of unauthorized modification of corrective action information can typically be addressed by basic procedures and controls. Recovery within hours, or even days, can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of corrective action information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for corrective action information is ***low***.

C.1.1.2 Program Evaluation Information Type

Program Evaluation involves the analysis of internal and external program effectiveness and the determination of corrective actions as appropriate. The recommended security categorization for the program evaluation information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

C.1.1.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of program evaluation information on the abilities of responsible agencies to analyze internal and external program effectiveness and to determine appropriate corrective actions. Unauthorized disclosure of program evaluation information can alert personnel associated with programs under evaluation to the focus and preliminary findings of investigative and evaluation activities. Armed with these

insights, program personnel can, in some cases, divert attention from questionable program attributes, hide unfavorable information, and make cosmetic changes that fail to correct underlying deficiencies but give false impressions to investigators and evaluators.

Special Factors Affecting Confidentiality Impact Determination: Where a major programs or human safety is at stake, actions taken based on unauthorized disclosure of program evaluation information can pose a threat to human life or a loss of major assets. In such cases, the confidentiality impact is ***high***. In any event, given the nature of program evaluation operations, it is anticipated that unauthorized disclosure of most program evaluation information often has the potential to seriously affect agency operations. Also, some program evaluation information, particularly in the case of current investigations, includes personal information subject to the Privacy Act of 1974 and/or information that is proprietary to a corporation or other organization.

Recommended Confidentiality Impact Level: Although there are many cases in which unauthorized disclosure of program evaluation information will have only a limited adverse effect on agency operations, assets, or individuals, the default confidentiality impact level recommended for program evaluation information is ***moderate***.

C.1.1.2.2 Integrity

The consequences of undetected unauthorized modification or destruction of program evaluation information can conceivably compromise the effectiveness of an evaluation program (e.g., by providing false information intended to mislead investigators or evaluators or to give program personnel a basis for claiming investigative or evaluative irregularities, thus supporting future challenges to program evaluation findings).

Special Factors Affecting Integrity Impact Determination: Given availability and use of basic procedures and controls, agency personnel can often recognize anomalous information and compare suspect information to that contained in original sources. The damage likely to be caused by unauthorized modification or destruction of program evaluation information is likely to be detected and corrected before it adversely affects agency operations or public confidence in the agency.

Recommended Integrity Impact Level: In general, the default integrity impact level assigned to program evaluation information is ***low***.

C.1.1.2.3 Availability

The effects of disruption of access to or use of program evaluation information can usually be repaired. The time frame required for repair is dependent on implementation and use of basic procedures and controls. Program evaluation processes are generally tolerant of reasonable delays.

Special Factors Affecting Availability Impact Determination: Availability and use of basic procedures and controls can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of program evaluation information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for program evaluation information is ***low***.

C.1.1.3 Program Monitoring Information Type

Program Monitoring involves the data-gathering activities required to determine the effectiveness of internal and external programs and the extent to which they comply with related laws, regulations, and policies. Subject to exception conditions described below, the recommended security categorization for the program monitoring information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

C.1.1.3.1 Confidentiality

The of confidentiality impact level is the effect of the unauthorized disclosure of program monitoring information on the ability of responsible agencies to perform those data-gathering activities required to determine the effectiveness of internal and external programs and the extent to which they comply with related laws, regulations, and policies.

Special Factors Affecting Confidentiality Impact Determination: Note that, as described in Section 3.1 above, *national security information* and *national security systems* are outside the scope of this guideline. Otherwise, where the data being collected belongs to one of the information types described in this guideline, the confidentiality impact assigned the data and system is that of the highest impact information type collected. Unauthorized disclosure of program monitoring information can alert personnel associated with programs being monitored to the focus and implications of monitoring activities. Armed with these insights, program personnel can, in some cases, divert attention from questionable program attributes, hide unfavorable information, and make cosmetic changes that fail to correct underlying deficiencies but give false impressions to monitors and evaluators. Where a major programs or human safety is at stake, actions taken based on unauthorized disclosure of program monitoring information can pose a threat to human life or a loss of major assets. In such cases, the confidentiality impact is ***high***.

Recommended Confidentiality Impact Level: Although there are many Federal environments in which unauthorized disclosure will have only a limited adverse effect on agency operations, assets, or individuals, there are enough circumstances in which serious adverse effects on agency operations, agency assets, or individuals can result to justify a ***moderate*** base confidentiality impact level for program monitoring information.

C.1.1.3.2 Integrity

The consequences of unauthorized modification or destruction of program monitoring information can compromise the effectiveness of the monitoring program. Most mitigating procedures and controls are designed to work with copies of data as it is collected and introduced into the system. In most cases, agency personnel cannot be expected to recognize anomalous monitoring information and compare suspect information to established baselines. The damage likely to be caused by unauthorized modification or destruction of program monitoring

information may very well adversely monitoring and evaluation results with consequent serious adverse effects on agency operations or public confidence in the agency.

Special Factors Affecting Integrity Impact Determination: The consequences can be particularly serious if the destruction or modification of monitoring information invalidates evaluation results concerning major programs or concerning threats to human safety. Once an integrity compromise has been detected, the adverse effects can often be corrected within reasonable time and resource constraints. The integrity impact resulting from unauthorized modification or deletion of program monitoring information depends in part on the nature of the laws or policies with which compliance is being determined and in part on the criticality of the processes being monitored. For example, in the case of safety regulations affecting manned space flight, the integrity impact level may be ***high***.

Recommended Integrity Impact Level: Although there are regulatory environments in which a ***high*** or ***moderate*** impact level is appropriate, the circumstances associated with most compliance monitoring suggests a ***low*** default integrity impact level.

C.1.1.3.3 Availability

The effects of disruption of access to or use of program monitoring information collected to determine the effectiveness of internal and external programs and the extent to which they comply with related laws, regulations, and policies can usually be repaired within reasonable time and resource constraints. The time and resources required for recovery is largely dependent on implementation and use of basic procedures and controls. In most cases, disruption of access to or use of program monitoring information is expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Not many compliance monitoring operations involve activities for which temporary loss of availability is likely to cause significant degradation in or loss of mission capability, place the agency at a significant disadvantage, result in major damage to or loss of major assets, or pose a threat to human life.

Recommended Availability Impact Level: The default availability impact recommended for program monitoring information is ***low***.

C.1.2 Regulatory Development

Regulatory Development involves activities associated with providing input to the lawmaking process in developing regulations, policies, and guidance to implement laws.

C.1.2.1 Policy and Guidance Development Information Type

Policy and Guidance Development involves the creation and dissemination of guidelines to assist in the interpretation and implementation of regulations. In most cases, the effect on public welfare of a loss of policy and guidance development mission capability can be expected to be delayed rather than immediate. As a result, the potential for consequent loss of human life or of major national assets is relatively low, since these most catastrophic consequences of impairment to mission capability can, in most cases, be corrected before they are fully realized. The

recommended security categorization for the policy and guidance development information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

C.1.2.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of policy and guidance information on the ability of responsible agencies to create and disseminate guidelines to assist in the interpretation and implementation of regulations.

Special Factors Affecting Confidentiality Impact Determination: The effects of loss of confidentiality of guidelines during the formative stage can result in attempts by affected entities and other interested parties to influence and/or impede the policy and guideline development process. Premature public release of formative policies and guidelines before internal coordination and review can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion. Delays can impair an agency's mission, but loss of public confidence can do serious and persistent harm to an agency's ability to effectively perform its mission.

Recommended Confidentiality Impact Level: The confidentiality default impact level recommended for policy and guidance development information is ***moderate***.

C.1.2.1.2 Integrity

The consequences of unauthorized modification or destruction of policy and guidance development information can generally be overcome if mitigating procedures and controls are adequate and are implemented and used. In most cases, competent agency personnel (e.g., authors and reviewers) should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain policy and guidance development information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. Note that public confidence consequences can be expected to be much more serious in cases of agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***.

Recommended Integrity Impact Level: However, in general, assuming the implementation and use of basic procedures and controls, the default integrity level recommended for policy and guidance development information is ***low***.

C.1.2.1.3 Availability

The effects of disruption of access to or use of policy and guidance development information or information systems can usually be repaired.

Special Factors Affecting Availability Impact Determination: The time frame required for repair is dependent on the use of basic procedures and controls, but the nature of policy and guidance development processes is usually tolerant of delays. Alternate communications media and retention of copies of source material can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Recommended Availability Impact Level: Assuming the implementation and use of basic back up and archiving procedures, the default availability impact level recommended for policy and guidance development information is normally ***low***.

C.1.2.2 Public Comment Tracking Information Type

Public Comment Tracking involves the activities of soliciting, maintaining, and responding to public comments regarding proposed regulations. Subject to exception conditions described below, the recommended security categorization for the public comment tracking information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1.2.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of public comment tracking information on the ability of responsible agencies to solicit, maintain, and respond to public comments regarding proposed regulations. The effects of loss of confidentiality of information associated with the public comment process is unlikely to pose the threat of serious harm to agency assets, personnel or operations.

Special Factors Affecting Confidentiality Impact Determination: In a few cases, the rationale for public comments can include information that is sensitive in terms of proprietary information sensitive Federal government information, or even national security information. However, such cases are exceptional and the information in question would be expected to be representative of information types covered elsewhere in this guideline.

Recommended Confidentiality Impact Level: The confidentiality default impact level recommended for public comment tracking information is ***low***.

C.1.2.2.2 Integrity

The consequences of unauthorized modification or destruction of public comment tracking information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel should be able to recognize anomalous public comment information and compare suspect information to that contained in source material. The sources of the suspect comments can always be contacted for verification purposes.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain public comment tracking information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: Assuming the implementation and use of basic procedures and controls the default integrity level recommended for public comment tracking information is ***low***.

C.1.2.2.3 Availability

The effects of disruption of access to or use of public comment tracking information or information systems can delay development of standards, guidelines, or regulations but can usually be repaired within reasonable time constraints.

Special Factors Affecting Availability Impact Determination: The time frame required for repair is dependent on use of basic mitigating procedures and controls, but the nature of public comment tracking processes is usually tolerant of delays. Alternate communications media and retention of copies of source material can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs. Permanent loss of comment information can disrupt some government operations by making it difficult to demonstrate due diligence in responses to comments, but this is more likely to take the form of delays in promulgation rather than of permanent damage.

Recommended Availability Impact Level: Assuming the implementation and use of basic procedures and controls, the default availability impact level recommended for public comment tracking information is normally ***low***.

C.1.2.3 Regulatory Creation Information Type

Regulatory Creation involves the activities of researching and drafting proposed and final regulations. Subject to exception conditions described below, the recommended security categorization for the regulatory creation information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

C.1.2.3.1 Confidentiality

The level of confidentiality impact level is the effect of unauthorized disclosure of regulatory creation information on the ability of responsible agencies to research and draft proposed and final regulations. The effects of loss of confidentiality of early drafts of regulations can result in attempts by affected entities and other affected parties to influence and/or impede the regulation development process. Premature public release of draft regulations before internal coordination and review has been conducted can result in unnecessary criticism of the proposed regulation and even damage public confidence in the agency.

Special Factors Affecting Confidentiality Impact Determination: These consequences are particularly likely where the release includes unedited internal commentary and discussion. Delays can impair an agency's mission, but loss of public confidence can do serious and persistent harm to an agency's ability to effectively perform its mission.

Recommended Confidentiality Impact Level: The confidentiality default impact level recommended for regulatory creation information is ***moderate***.

C.1.2.3.2 Integrity

The consequences of unauthorized modification or destruction of regulatory creation information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel (e.g., authors and reviewers) should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain regulatory information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. Note that public confidence consequences can be expected to be much more serious in cases of agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***.

Recommended Integrity Impact Level: In general, assuming the implementation and use of basic procedures and controls, the default integrity level recommended for regulatory creation information is ***low***.

C.1.2.3.3 Availability

The effects of disruption of access to or use of regulatory creation information or information systems can usually be repaired.

Special Factors Affecting Availability Impact Determination: The time frame required for repair is dependent on mitigating procedures and controls, but the nature of regulatory creation processes is usually tolerant of delays. Procedures and controls, such as alternate communications media and retention of copies of source material, can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Recommended Availability Impact Level: Assuming the implementation and use of basic back up and archiving procedures, the default availability impact level recommended for regulatory creation information is normally ***low***.

C.1.2.4 Rule Publication Information Type

Rule Publication includes the all activities associated with the publication of a proposed or final rule in the Federal Register and Code of Federal Regulations. Subject to exception conditions described below, the recommended security categorization for the rule publication information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1.2.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of rule publication information on the ability of responsible agencies to publish proposed or final rules in the

Federal Register and Code of Federal Regulations. The published rules are, by definition, public information.

Special Factors Affecting Confidentiality Impact Determination: The effects of loss of confidentiality of information associated with the rule publication process is unlikely to pose the threat of serious harm to agency assets, personnel or operations.

Recommended Confidentiality Impact Level: In general, the default confidentiality impact level recommended for rule publication information is ***low***.

C.1.2.4.2 Integrity

The consequences of unauthorized modification or destruction of rule publication information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel (e.g., authors and reviewers) should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: In the worst cases, *errata* can be published. Unauthorized modification or destruction of information may result in unnecessary expenditures, some confusion, and limited damage to public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: In general, assuming the implementation and use of basic procedures and controls, the default integrity level recommended for rule publication information is ***low***.

C.1.2.4.3 Availability

The effects of disruption of access to or use of rule publication information or information systems can usually be repaired.

Special Factors Affecting Availability Impact Determination: The time frame required for repair is dependent on employment of mitigating procedures and controls, but the nature of rule publication processes is usually tolerant of delays.

Recommended Availability Impact Level: Assuming the implementation and use of basic procedures and controls, the default availability impact level recommended for rule publication information is normally ***low***.

C.1.3 Planning and Resource Allocation

Planning and Resource Allocation involves the activities of determining strategic direction, identifying and establishing programs and processes to enable change, and allocating resources (capital and labor) among those programs and processes.

C.1.3.1 Budget Formulation Information Type

Budget Formulation involves all activities undertaken to determine priorities for future spending and to develop an itemized forecast of future funding and expenditures during a targeted period

of time. This includes the collection and use of performance information to assess the effectiveness of programs and develop budget priorities. Subject to exception conditions described below, the recommended security categorization for the budget formulation information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

C.1.3.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of budget formulation information on the ability of responsible agencies to determine priorities for future spending and to develop an itemized forecast of future funding and expenditures during a targeted period of time. The effects of loss of confidentiality of information on the basis on which budgets are developed, or of early drafts of budgets, can result in attempts by competing interests to influence and/or impede the regulation development process. The consequences to agency programs and even of the ability of an agency to perform its mission can be very serious. Premature public release of draft budgets before internal coordination and review has been conducted can result in unnecessary criticism of the proposed regulation and even damage public confidence in the agency. These consequences are particularly likely where the release includes unedited internal commentary and discussion. Delays that result from confidentiality compromise can imperil specific agency programs, but loss of public confidence can do persistent harm to an agency's ability to effectively perform its mission.

Special Factors Affecting Confidentiality Impact Determination: Note that some budget information of some Federal agencies is classified *national security information*. Such information, while extremely sensitive is outside the scope of this guideline.

Recommended Confidentiality Impact Level: Based on the serious harm that can be suffered by an agency due to unauthorized disclosure of draft budget information (and associated commentary), the default confidentiality impact level recommended for budget formulation information is ***moderate***.

C.1.3.1.2 Integrity

The consequences of unauthorized modification or destruction of budget formulation information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel (e.g., authors and reviewers) should be able to recognize anomalous budget information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain budget information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. Note that public confidence consequences can be expected to be much more serious in cases of agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***.

Recommended Integrity Impact Level: Assuming the implementation and use of basic procedures and controls, the default integrity level recommended for budget formulation information is ***low***.

C.1.3.1.3 Availability

The effects of disruption of access to or use of budget formulation information or information systems can usually be repaired.

Special Factors Affecting Availability Impact Determination: The time frame required for repair is dependent on the adequacy of mitigating procedures and controls, but the nature of budget formulation processes is usually tolerant of delays. Excessive recovery delays can result in loss of funding.

Recommended Availability Impact Level: Assuming the implementation and use of basic procedures and controls, the default availability impact level recommended for budget formulation information is normally ***low***.

C.1.3.2 Capital Planning Information Type

Capital Planning involves the processes for ensuring that appropriate investments are selected for capital expenditures. The recommended default security categorization for capital planning information is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1.3.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of capital planning information on the ability of responsible agencies to ensure that appropriate investments are selected for capital expenditures. The effects of loss of confidentiality of capital investment plans during the formative stage can result in attempts by affected entities and other interested parties to influence and/or impede the policy and guideline development process. Premature public release of draft plans before internal coordination and review can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion. The diversion of investment funds that can result from compromise of draft plans can pervert investment priorities in a manner that is prejudicial to public interest.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some of the background information that supports development of capital investment plans can reveal sensitive vulnerabilities, capabilities, or methods of anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some capital investment plans of some Federal agencies contain *national security information*. However, the consequence of loss of confidentiality of most capital planning information is likely to do only limited harm to government assets, personnel, or missions.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for capital planning information is ***low***.

C.1.3.2.2 Integrity

The consequences of unauthorized modification or destruction of capital planning information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel (e.g., authors and reviewers) should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain capital planning information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. Note that public confidence consequences can be expected to be much more serious in cases of agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***. Similar damage is likely to result from exposure to the public of modified information before the modification has been detected.

Recommended Integrity Impact Level: Assuming the implementation and use of basic procedures and controls, the default integrity level recommended for capital planning information is ***low***.

C.1.3.2.3 Availability

The effects of disruption of access to or use of capital planning information or information systems can usually be repaired.

Special Factors Affecting Availability Impact Determination: The time frame required for repair is dependent on employment of basic procedures and controls, but the nature of capital planning processes is usually tolerant of delays. Basic procedures and controls can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Recommended Availability Impact Level: Assuming the implementation and use of basic procedures and controls, the default availability impact level recommended for capital planning information is ***low***.

C.1.3.3 Enterprise Architecture Information Type

Enterprise Architecture is an established process for describing the current state and defining the target state and transition strategy for an organizations people, processes, and technology. The recommended default security categorization for the enterprise architecture information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1.3.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of enterprise architecture information on the ability of responsible agencies to describe the current state and define the target state and transition strategy for an organizations people, processes, and technology. The effects of loss of confidentiality of preliminary draft enterprise architecture plans can result in attempts by affected entities and other interested parties to influence and/or impede the policy and guideline development process. Premature public release of draft plans before internal coordination and review can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some of the background information that supports development of Federal enterprise architecture can reveal sensitive vulnerabilities, capabilities, or methods of anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some enterprise architecture plans of some Federal agencies are themselves *national security information*. However, the consequence of loss of confidentiality of most enterprise architecture information is likely to do only limited harm to government assets, personnel, or missions.

Recommended Availability Impact Level: The default confidentiality impact level recommended for enterprise architecture information is ***low***.

C.1.3.3.2 Integrity

The consequences of unauthorized modification or destruction of enterprise architecture information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain enterprise architecture information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. Note that public confidence consequences can be expected to be much more serious in cases of agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***. Similar damage is likely to result from exposure to the public of modified information before the modification has been detected.

Recommended Availability Impact Level: In general, assuming the implementation and use of basic procedures and controls, the default integrity level recommended for enterprise architecture information is ***low***.

C.1.3.3.3 Availability

The effects of disruption of access to or use of enterprise architecture information or information systems can usually be repaired. The time frame required for repair is dependent on the mitigating procedures and controls, but the nature of enterprise architecture processes is usually tolerant of delays. Rigorous employment of basic procedures and controls can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Recommended Availability Impact Level: Assuming the implementation and use of basic procedures and controls, the default availability impact level recommended for enterprise architecture information is ***low***.

C.1. 3.4 Strategic Planning Information Type

Strategic Planning entails the determination of long-term goals and the identification of the best approach for achieving those goals. The recommended default security categorization for strategic planning information is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1.3.4.1 Confidentiality

The confidentiality impact level is the effect of the unauthorized disclosure of strategic planning information on the ability of responsible agencies to determine long-term goals and to identify of the best approach for achieving those goals. Premature public release of draft plans before internal coordination and review can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some of the background information that supports development of some Federal strategic plans can reveal sensitive vulnerabilities, capabilities, or methods of anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some strategic plans are themselves *national security information*. However, the consequence of loss of confidentiality of most strategic planning information is likely to do only limited harm to government assets, personnel, or missions.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for strategic planning information is ***low***.

C.1.3.4.2 Integrity

The consequences of unauthorized modification or destruction of strategic planning information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain strategic planning information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. Note that public confidence consequences can be expected to be much more serious in cases of agencies that have national defense, intelligence, or information security missions. In such cases, the impact may be at least ***moderate***. Similar damage is likely to result from exposure to the public of modified information before the modification has been detected.

Recommended Integrity Impact Level: In general, assuming the implementation and use of basic procedures and controls, the default integrity level recommended for strategic planning information is ***low***.

C.1.3.4.3 Availability

The effects of disruption of access to or use of strategic planning information or information systems can usually be repaired. The time frame required for repair is dependent on employment of basic procedures and controls, but the nature of strategic planning processes is usually tolerant of delays.

Special Factors Affecting Availability Impact Determination: Mitigating procedures and controls can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Recommended Availability Impact Level: Assuming the implementation and use of basic procedures and controls, the availability impact level associated with strategic planning information is normally ***low***.

C.1.3.5 Budget Execution Information Type

Budget Execution involves day-to-day requisitions and obligations for agency expenditures, invoices, billing dispute resolution, reconciliation, service level agreements, and distributions of shared expenses. The recommended default security categorization for budget execution information is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)}

C.1.3.5.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of budget execution information on the ability of responsible agencies to manage day-to-day requisitions and obligations for agency expenditures, invoices, billing dispute resolution, reconciliation, service level agreements, and distributions of shared expenses.

Special Factors Affecting Confidentiality Impact Determination: The effects of loss of confidentiality of budget execution information can violate privacy regulations, reveal information proprietary to private institutions, and procurement-sensitive information. In aggregate, budget execution information can reveal capabilities and methods that some agencies

(e.g., law enforcement, homeland security, national defense, intelligence) consider extremely sensitive. In these cases, the potential harm that can result from unauthorized disclosure ranges from ***moderate*** to ***high*** to *national security-related*. In the last case, the information is outside the scope of this document. Public release of sensitive budget execution information can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion. However, the consequence of loss of confidentiality of most budget execution information is likely to do serious harm to government assets, personnel, or missions.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for budget execution information is ***moderate***.

C.1.3.5.2 Integrity

The consequences of unauthorized modification or destruction of budget execution information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Where small dollar amounts are modified, the potential damage to an agency's mission that one would expect to result from delayed discovery of an integrity compromise is limited and can generally be corrected within reasonable time and resource constraints. However, in the case of agreements or transactions involving large monetary values, asset losses, immediate damage to agency operations, and potential for serious and persistent loss of public confidence can be expected to be serious to catastrophic. The consequent integrity risk is ***moderate*** to ***high***. There may very well be on-line, automated, or semi-automated activities for which integrity threats can be realized before they are detected. Procedures are in place in most responsible agencies to mitigate the effects of these consequences. Where unauthorized modification or destruction of other collection of revenue information facilitates or enables a catastrophic confidentiality or availability risk scenario, the integrity risk level may be ***high***.

Recommended Integrity Impact Level: In general, the default integrity level recommended for budget execution information is ***moderate***.

C.1.3.5.3 Availability

The effects of disruption of access to or use of budget execution information or information systems can usually be repaired. The time frame required for repair is dependent on procedures and controls, but the nature of budget execution processes is usually tolerant of delays.

Special Factors Affecting Availability Impact Determination: Mitigating procedures and controls can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Recommended Availability Impact Level: Assuming the implementation and use of basic procedures and controls, the availability impact level associated with budget execution information is normally ***low***.

C.1.3.6 Workforce Planning Information Type

Workforce Planning involves the processes for identifying the workforce competencies required to meet the agency's strategic goals and for developing the strategies to meet these requirements. The recommended security categorization for workforce planning information is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1.3.6.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of workforce planning information on the ability of responsible agencies to identify workforce competencies required to meet the agency's strategic goals and for developing the strategies to meet these requirements. It is anticipated that unauthorized disclosure of most workforce planning information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some of the background information that supports development of some Federal workforce plans can reveal sensitive vulnerabilities, tables of organization, capabilities, or methods of anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline).

Recommended Confidentiality Impact Level: The base confidentiality impact level assigned to workforce planning information is ***low***.

C.1.3.6.2 Integrity

The consequences of undetected unauthorized modification or destruction of workforce planning information can conceivably compromise the effectiveness of compliance enforcement actions (e.g., by providing violators with a basis for claiming investigative or enforcement irregularities, thus supporting legal challenges to proposed workforce plans). However, given availability and use of basic procedures and controls, agency personnel can usually be expected to recognize anomalous information and compare suspect information to that contained in original sources. The damage likely to be caused by unauthorized modification or destruction of workforce planning information is likely to be detected and corrected before it adversely affects agency operations or public confidence in the agency.

Recommended Integrity Impact Level: In general, the base integrity impact level assigned to workforce planning information is ***low***.

C.1.3.6.3 Availability

The effects of disruption of access to or use of workforce planning information can usually be repaired. The time frame required for repair is dependent on implementation and use of basic procedures and controls. Workforce planning processes are generally tolerant of reasonable delays. Availability and use of alternate facilities can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of workforce planning information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: Therefore, the default availability impact recommended for workforce planning information is ***low***.

C.1.3.7 Management Improvement Information Type

Management Improvement includes all efforts to gauge the ongoing efficiency of business processes and identify opportunities for reengineering or restructuring. The recommended default security categorization for the management improvement information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1.3.7.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of management improvement information on the ability of responsible agencies to gauge the ongoing efficiency of business processes and identify opportunities for reengineering or restructuring. Premature public release of draft plans before internal coordination and review can result in unnecessary damage to public confidence in the agency. This is particularly likely where the release includes unedited internal commentary and discussion.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some of the background information that supports development of some Federal management improvement plans can reveal personnel-sensitive information, including some information subject to the Privacy Act of 1974. Other background information can reveal sensitive vulnerabilities, capabilities, or methods of anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some strategic plans are themselves *national security information*. However, the consequence of loss of confidentiality of most management improvement information is likely to involve only limited harm to government assets, personnel, or missions.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for management improvement information is ***low***.

C.1.3.7.2 Integrity

The consequences of unauthorized modification or destruction of management improvement information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain management improvement information (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. Note that public confidence consequences can be expected to be much more serious in cases of agencies that have national defense, intelligence, or information security missions. In such cases, the impact may

be at least ***moderate***. Similar damage is likely to result from exposure to the public of modified information before the modification has been detected. Failure to detect malicious modification of personnel information (mostly background information) can result in disruption of some agency operations and even disruptive and harmful administrative or legal actions.

Recommended Integrity Impact Level: In general, assuming the implementation and use of basic procedures and controls, the default integrity level recommended for management improvement information is ***low***.

C.1.3.7.3 Availability

The effects of disruption of access to or use of management improvement information or information systems can usually be repaired. The time frame required for repair is dependent on procedures and controls, but the nature of management improvement planning processes is usually tolerant of delays.

Special Factors Affecting Availability Impact Determination: Implementation and use of mitigating procedures and controls can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Recommended Availability Impact Level: Assuming the implementation and use of basic procedures and controls, the availability impact level associated with management improvement information is normally ***low***.

C.1.4 Internal Risk Management and Mitigation

Internal risk management and mitigation involves all activities relating to the processes of analyzing exposure to risk and determining appropriate counter-measures. Note that risks to much information and many information systems associated with many internal risk management and mitigation activities may inherently affect the resistance to compromise/damage and recovery from damage with respect to a broad range of critical infrastructures and key national assets.

C.1.4.1 Contingency Planning Information Type

Contingency planning involves the actions required to plan for, respond to, and mitigate damaging events. The recommended default security categorization for the contingency planning information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, MODERATE)}

C.1.4.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of contingency planning information on the ability of responsible agencies to plan for, respond to, and mitigate damaging events. Unauthorized disclosure of contingency planning information may equip an adversary with the information necessary to attack a system in such a way that recovery is impaired or even blocked. Such information can be the basis for availability impact of an attack to increase from ***low*** to ***high***.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some of the assumptions and other background information that supports development of some Federal contingency plans can reveal sensitive vulnerabilities, capabilities, intelligence assessments, intelligence sources, or methods employed in anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some contingency plans are themselves *national security information*. However, the purpose of most contingency planning information is to protect against inadvertent or accidental damaging events rather than against malicious attacks. Even so, in the case of Federal government systems, the case of hostile attacks on systems must be considered. As a result, it must be assumed that the consequence of loss of confidentiality of most contingency planning information is likely to do serious harm to government assets, personnel, or missions.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for contingency planning information is ***moderate***.

C.1.4.1.2 Integrity

The consequences of unauthorized modification or destruction of contingency planning information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Recommended Integrity Impact Level: In general, assuming the implementation and use of basic procedures and controls, the default integrity level recommended for contingency planning information is ***low***.

C.1.4.1.3 Availability

The effects of disruption of access to or use of contingency planning information or information systems depend on the timing of the disruption. Access disruption at the time of an outage can delay recovery and significantly increase the harm caused by information systems disruption to government agencies. The time frame required for repair is dependent on adequacy and accessibility of procedures and controls, and on the familiarity of key personnel with the location and employment of the procedures.

Special Factors Affecting Availability Impact Determination: While the nature of contingency planning processes is usually tolerant of delays, that of the contingency plan implementation process is not. The consequences depend on both the period of the outage and the criticality of the disrupted processes. The consequent impact level can range from ***low*** to ***high***.

Recommended Availability Impact Level: The default availability impact level recommended for contingency planning information should be considered to be at least ***moderate***.

C.1.4.2 Continuity of Operations Information Type

Continuity of operations involves the activities associated with the identification of critical systems and processes, and the planning and preparation required to ensure that these systems

and processes will be available in the event of a catastrophic event. The recommended default security categorization for the continuity of operations information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, MODERATE)}

C.1.4.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of continuity of operations information on the ability of responsible agencies to identify critical systems and processes, and to conduct the planning and preparation required to ensure that these systems and processes will be available in the event of a catastrophic event. Unauthorized disclosure of continuity of operations information may inform an adversary regarding what facilities and processes are considered to be critical. Such unauthorized disclosure may also equip an adversary with the information necessary to attack a system in such a way that operations are disrupted, and that recovery is impaired or even blocked. Such information can be the basis for availability impact of an attack to increase from ***low*** to ***high***.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some of the assumptions and other background information that supports development of some Federal contingency plans can reveal sensitive vulnerabilities, capabilities, intelligence assessments, intelligence sources, or methods employed in anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some contingency plans are themselves *national security information*. However, the purpose of most continuity of operations information is to protect against inadvertent or accidental damaging events rather than against malicious attacks. Even so, in the case of Federal government systems, the case of hostile attacks on systems must be considered. As a result, it must be assumed that the consequence of loss of confidentiality of most continuity of operations information is likely to do serious harm to government assets, personnel, or missions.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for continuity of operations information is ***moderate***.

C.1.4.2.2 Integrity

The consequences of unauthorized modification or destruction of continuity of operations information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Recommended Integrity Impact Level: In general, assuming the implementation and use of basic procedures and controls, the default integrity level recommended for continuity of operations information is ***low***.

C.1.4.2.3 Availability

The effects of disruption of access to or use of continuity of operations information or information systems depend on the timing of the disruption. Access disruption at the time of an

outage can delay recovery and significantly increase the harm caused by information systems disruption to government agencies. The time frame required for repair is dependent on adequacy and accessibility of procedures and controls, and on the familiarity of key personnel with the location and employment of the procedures.

Special Factors Affecting Availability Impact Determination: While the nature of continuity of operations processes is usually tolerant of delays, that of the contingency plan implementation process is not. The consequences depend on both the period of disruption of operations and the criticality of the disrupted processes. The consequent impact level can range from ***low*** to ***high***.

Recommended Availability Impact Level: In general, the default availability impact level associated with continuity of operations information should be considered to be at least ***moderate***.

C.1.4.3 Service Recovery Information Type

Service recovery involves the internal actions necessary to develop a plan for resuming operations after a catastrophe occurs, such as a fire or earthquake. The recommended default security categorization for the service recovery information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1.4.3.1 Confidentiality

The confidentiality impact level is the effect of the unauthorized disclosure of service recovery information on the ability of responsible agencies to develop plans for resuming operations after a catastrophe occurs, such as a fire or earthquake. In the case of service recovery plans for natural catastrophes, the information associated with service recovery planning is not intrinsically sensitive. In the case of catastrophes caused by malicious activity, unauthorized disclosure of service recovery information may inform an adversary regarding what facilities and processes are considered to be critical. Such unauthorized disclosure may also equip an adversary with the information necessary to attack a system in such a way that operations are disrupted, and that recovery is impaired or even blocked. Such information can be the basis for increasing the availability impact of an attack from ***low*** to ***high***.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some of the assumptions and other background information that supports development of some Federal service recovery plans can reveal sensitive vulnerabilities, capabilities, intelligence assessments, intelligence sources, or methods employed in anti-terrorism, law enforcement, or national security activities. Depending on the information in question, the confidentiality impact can be ***moderate, high***, or involve *national security information* (outside the scope of this guideline). Also, some service recovery plans are themselves *national security information*. However, the purpose of most service recovery information is to protect against natural catastrophes rather than against malicious attacks. In most cases, the consequence of loss of confidentiality of service recovery information is not likely to do serious harm to government assets, personnel, or missions.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for service recovery information is ***low***.

C.1.4.3.2 Integrity

The consequences of unauthorized modification or destruction of service recovery planning information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Recommended Integrity Impact Level: In general, assuming the implementation and use of basic procedures and controls, the default integrity level recommended for service recovery planning information is ***low***.

C.1.4.3.3 Availability

The effects of disruption of access to or use of service recovery information or information systems depend on the timing of the disruption. The effects of access disruption during the planning process itself can usually be repaired. The time frame required for repair is dependent on procedures and controls, but the nature of service recovery planning processes is usually tolerant of delays. Alternate communications media and retention of copies of source material can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Special Factors Affecting Availability Impact Determination: Disruption of access to service recovery plans at the time of an outage can delay recovery and significantly increase the harm caused by information systems disruption to government agencies. The time frame required for repair is dependent on adequacy and accessibility of procedures and controls, and on the familiarity of key personnel with the location and employment of the recovery procedures. While the nature of service recovery planning is usually tolerant of delay, that of implementation of recovery plans is not. In the case of recovery plan implementation, the consequences of access disruption depend on both the period of disruption of operations and the criticality of the disrupted processes. The consequent impact level can range from ***low*** to ***high***.

Recommended Availability Impact Level: The default availability impact level recommended for service recovery planning information during the planning process is ***low***.

C.1.5 Revenue Collection

Revenue Collection includes the collection of Government income from all sources. Note: Tax collection is accounted for under the Taxation Management information type in the General Government mission area.

C.1.5.1 Debt Collection Information Type

Debt Collection supports activities associated with the collection of money owed to the United States government from both foreign and domestic sources. The recommended security categorization for debt collection information is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

C.1.5.3.1 Confidentiality

The confidentiality risk level is the effect of unauthorized disclosure of debt collection information on the ability of responsible agencies to properly and efficiently collect money owed to the United States government from both foreign and domestic sources. The consequences of unauthorized disclosure of debt collection information are generally dependent on the identity of the debtor and of the nature and value of the debt being collected. Where the amount of the debt is significant, and advance or otherwise unauthorized knowledge regarding the collection of a debt by coercive means (e.g., tort or seizure) might imperil successful collection, then the associated confidentiality risk assigned to personal property management information might be ***moderate*** (or even ***high*** in the case of extremely high dollar value cases). However, it is anticipated that unauthorized disclosure of most debt collection information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974, information that is proprietary to a corporation or other organization, or information that is considered to be politically sensitive by a foreign government. Such information will often be associated with debt collection processes.

b. Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for debt collection information is ***moderate***.

C.1.5.3.2 Integrity

The consequences of unauthorized modification to or destruction of debt collection information depends, not only on the nature of the property being managed, but also on the immediacy with which the information is expected to be used. The consequences of unauthorized modification or destruction of debt collection information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: In the case of delayed discovery of modified information or destruction of information that is not backed up, if the modified or destroyed information is substantive in a financial sense, there is a greater potential for harm to result from actions being taken based on incomplete or false information. This can have serious adverse effects on individual financial actions with consequent loss of revenue from, or other unanticipated consequences regarding the personal property under disposition. The severity of the consequent integrity risk depends on the nature of the debt and of the debtor entity (see Appendix C.1.5.3.1), but would be most likely be ***moderate***.

Recommended Integrity Impact Level: Assuming availability and diligent use of basic mitigating procedures and controls, the default availability impact level associated with most debt collection information is ***low***.

C.1.5.3.3 Availability

The effects of disruption of access to or use of debt collection information or information systems can likely be repaired in time to prevent serious loss. The time frame required for repair is dependent on procedures and controls, but the nature of most Federal debt collection processes is generally tolerant of delays. The consequences of temporary inability to access or information concerning foreign or domestic debt would be negligible.

Recommended Availability Impact Level: The default availability risk recommended for most debt collection information is ***low***.

C.1.5.2 User Fee Collection Information Type

User fee Collection involves the collection of fees assessed on individuals or organizations for the provision of Government services and for the use of Government goods or resources (i.e. National Parks). The recommended security categorization for the user fee collection information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, MODERATE)}

C.1.5.2.1 Confidentiality

The confidentiality risk level is the effect of unauthorized disclosure of user fee collection information on the ability of responsible agencies to correctly and efficiently enforce, regulate, and effect the collection of fees assessed on individuals or organizations for the provision of Government services and for the use of Government goods or resources. In general, particularly in aggregate, this information is public record.

Recommended Confidentiality Impact Level: The recommended default confidentiality risk level for user fee collection information is ***low***.

C.1.5.2.2 Integrity

There may be circumstances under which unauthorized modification to or destruction of user fee collection information is undertaken as part of a scheme to divert payments, conceal underpayment of failure to make payment of fees, or otherwise defraud the government. As for other information types, the consequences of unauthorized modification to or destruction of user fee collection information depends, not only on the adequacy and rigorous implementation of basic procedures and controls, but on the urgency with which the information is normally needed. The consequences of unauthorized modification or destruction of user fee collection information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications might conceivably have an adverse effect on agency operations, image and reputation. There may be on-line, automated, or semi-automated activities for which integrity threats can be realized before they are detected. Procedures are in place in most responsible agencies to mitigate the effects of these consequences.

Recommended Integrity Impact Level: The default integrity risk level recommended for user fee collection information is ***low***.

C.1.5.2.3 Availability

The effects of disruption of access to or use of unauthorized modification to or destruction of user fee collection information or information systems can usually be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on procedures and controls, and the nature of missions supported by user fee collection information is somewhat tolerant of delay. Alternate communications media and retention of copies of source material can usually be depended on to prevent significant degradation in mission capability and resultant serious or catastrophic consequences. Any extended period of unavailability would likely be seriously disruptive to the operations for which fees are collected.

Recommended Availability Impact Level: The availability risk level recommended for other collection of revenue information is ***moderate***.

C.1.5.3 Federal Asset Sales Information Type

Federal Asset Sales encompasses the activities associated with the acquisition, oversight, tracking, and sale of non-internal assets managed by the Federal Government with a commercial value and sold to the private sector. The recommended security categorization for the Federal asset sales information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

C.1.5.3.1 Confidentiality

The confidentiality risk level is the effect of the unauthorized disclosure of Federal asset sales information on the ability of responsible agencies to properly and efficiently acquire, oversee, track, and sell non-internal assets managed by the Federal Government with a commercial value and sold to the private sector. The consequences of unauthorized disclosure of Federal asset sales information are generally dependent on the nature and value of the property being disposed. Generally, Federal asset sales information is both officially, and intended to be, public. Most managed property would not be of sufficient individual value to occasion such an occurrence (bid rigging, etc.). Reasonable controls over unauthorized disclosure of Federal asset sales information should be adequate, and no serious consequences could reasonably be expected to result.

Special Factors Affecting Confidentiality Impact Determination: Where advance or otherwise unauthorized knowledge regarding the property being disposed of might lead to unfair advantage (i.e., ability to accurately bid on an auction lot to the detriment of other bidders), then the associated confidentiality risk assigned to personal property management information might be ***moderate***. Such an instance might arise if a disruption of the proper procedures could reasonably cause an adverse effect on future operations of the responsible agency, or if the agency's image, or individual reputations might be damaged.

Recommended Confidentiality Impact Level: The default confidentiality risk recommended for most Federal asset sales information is ***low***.

C.1.5.3.2 Integrity

The consequences of unauthorized modification to or destruction of Federal asset sale information depends, not only on the nature of the property being managed, but also on the immediacy with which the information is expected to be used. The consequences of unauthorized modification or destruction of Federal asset sale information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, solicitations for bid, official notices of disposition, etc.) may potentially adversely affect operations, image or reputation, but the damage to the management mission would usually be of more immediate concern. If the modified or destroyed information is substantive in a financial sense, there is a greater potential for actions being taken based on incomplete or false information. This can have serious adverse effects on individual financial actions with consequent loss of revenue from, or other unanticipated consequences regarding the personal property under disposition. The severity of the consequent integrity impact depends on the nature of the property (see Appendix C.1.5.3.1), but would be most likely be ***moderate***.

Recommended Integrity Impact Level: The default integrity impact level recommended for Federal asset sales information is ***moderate***.

C.1.5.3.3 Availability

The effects of disruption of access to or use of Federal asset sale information or information systems can likely be repaired in time to prevent serious loss. The time frame required for repair is dependent on procedures and controls, but the nature of missions supported by Federal asset sale information is generally tolerant of delays. The consequences of temporary inability to access or promulgate solicitations for bid, official notices of disposition, etc., would be negligible.

Recommended Availability Impact Level: The default availability risk recommended for most Federal asset sale information is ***low***.

C.1.6 Public Affairs

Public Affairs activities involve the exchange of information and communication between the Federal Government, citizens and stakeholders in direct support of citizen services, public policy, and/or national interest.

C.1.6.1 Customer Services Information Type

Customer Service supports activities associated with providing and managing the delivery of information and support to the government's customers. The recommended security categorization for the customer service information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1. 6.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of customer service information on the ability of responsible agencies to provide and manage the delivery of information and support to the government's customers. Most customer service information is likely to be in the public domain and poses no confidentiality impact.

Special Factors Affecting Confidentiality Impact Determination: Some customer service information may include customer-provided information covered by the provisions of the Privacy Act of 1974. Unauthorized disclosure of large volumes of information protected under the Privacy Act can be expected to have a serious to severe effect on public confidence in the agency. Actions taken that are intended to establish blame, compensate victims, or repair damage done with the exposed information can cause serious disruption of an agency's mission capability. In such cases, the confidentiality impact can be ***moderate***. Use of customer waiver of Privacy Act protection can mitigate some of this impact. Additionally, some customer services information (e.g., information contained in on-line security clearance requests) may be considered sensitive by both individuals and sponsoring organizations independent of Privacy Act considerations). However, in most cases, unauthorized disclosure of customer service information will have at most a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for customer service information is ***low***.

C.1. 6.1.2 Integrity

Customer service activities are not generally time-critical. The consequences of unauthorized modification of customer service information can generally be overcome if basic procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: An increasing proportion of customer service activities are interactive. There is, therefore, a potential for customer actions being taken based on modified or incomplete information. Similarly, unauthorized modification or deletion of customer-supplied information can result in government mishandling of interactions with customers. If this occurs on a large scale (e.g., many Social Security Administration interactions), serious damage to public confidence in the agency may result, and the extensive corrective actions that may be required can place the agency at a significant disadvantage. In such cases, a ***moderate*** integrity may be associated with customer service information. This becomes increasingly common as E-government initiatives progress. Also, unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to most missions would usually be limited. However, in most current cases, the adverse effects of unauthorized modification to or destruction of customer service information on overall agency mission functions or public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for customer service information is ***low***.

C.1. 6.1.3 Availability

The effects of disruption of access to or use of customer service information can usually be repaired. The time frame required for repair is dependent on implementation and use of basic procedures and controls. However, customer service processes are not reliably tolerant of delay. Availability and use of back-up files and alternate facilities can usually prevent long term or permanent damage to mission capability, but restoration of service is unlikely to occur in real time. Even temporary loss of availability of customer service information is likely to disrupt customer operations.

Special Factors Affecting Availability Impact Determination: While most outages will result in only limited adverse effects on government operations, repeated outages can have a serious adverse effect on public confidence in the agency. In such cases, the availability impact might be ***moderate***.

Recommended Availability Impact Level: In most cases, though, disruption of access to or use of customer service information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals. Therefore, the default availability impact recommended for customer service information is ***low***.

C.1.6.2 Official Information Dissemination Information Type

Official Information Dissemination includes all efforts to provide official government information to external stakeholders through the use of various types of media, such as video, paper, web, etc. The recommended security categorization for the official information dissemination information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1. 6.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of official information dissemination information on the ability of responsible agencies to provide official Federal government information to external stakeholders through the use of various communications media. Official information dissemination information is almost always in the public domain and poses no confidentiality impact.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for official information dissemination information is ***low***.

C.1. 6.2.2 Integrity

Official information dissemination activities are not usually time-critical. The consequences of unauthorized modification of official information dissemination information can generally be overcome if review procedures are in place and basic procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare

suspect information to that contained in source material. On the other hand, there is a potential for customer actions being taken based on modified or incomplete information. Also, unauthorized modification or destruction of official information dissemination information that is not immediately detected can result in distribution of false and misleading information (e.g., modified web pages, electronic mail, video). Such events can be expected to adversely affect operations or public confidence in the agency. This can significantly degrade the official information dissemination mission capability. In such cases, a ***moderate*** integrity impact may exist.

Special Factors Affecting Integrity Impact Determination: The more serious integrity impacts become increasingly likely as E-government initiatives progress.

Recommended Availability Impact Level: In most current cases, the adverse effects of unauthorized modification to or destruction of official information dissemination information on overall agency mission functions is expected to be limited. Therefore, the default integrity impact recommended for official information dissemination information is ***low***.

C.1. 6.2.3 Availability

The effects of disruption of access to or use of official information dissemination information can usually be repaired. The time frame required for repair is dependent on implementation and use of basic procedures and controls. Official information dissemination processes are generally tolerant of limited delays. Availability and use of back-up files and alternate facilities can usually prevent long term or permanent damage to mission capability. However, even temporary loss of availability of official information dissemination information is likely to have an adverse effect on public confidence in the agency.

Special Factors Affecting Availability Impact Determination: While most cases will result in only limited consequences, repeated outages can have a serious adverse effect on public confidence in the agency. This can significantly degrade the official information dissemination mission capability. In such cases, the availability impact might be ***moderate***.

Recommended Availability Impact Level: In most cases, though, disruption of access to or use of official information dissemination information can be expected to have only a limited adverse effect on overall agency operations, agency assets, or individuals. Therefore, the default availability impact recommended for official information dissemination information and information systems is ***low***.

C.1.6.3 Product Outreach Information Type

Product Outreach relates to the marketing of government services products, and programs to the general public in an attempt to promote awareness and increase the number of customers/beneficiaries of those services and programs. The recommended security categorization for the product outreach information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1. 6.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of product outreach information on the ability of responsible agencies to market government services products, and programs to the general public in an attempt to promote awareness and increase the number of customers/beneficiaries of those services and programs. Product outreach information is almost always in the public domain and poses no confidentiality impact.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for product outreach information is ***low***.

C.1. 6.3.2 Integrity

Product outreach activities are not usually time-critical. The consequences of unauthorized modification of product outreach information can generally be overcome if review procedures are in place and basic procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material. On the other hand, unauthorized modification or destruction of product outreach information that is not immediately detected can result in distribution of false and misleading information. Such events can be expected to adversely affect operations or public confidence in the agency. This can significantly degrade the product marketing mission capability. In such cases, a ***moderate*** integrity impact may exist.

Recommended Integrity Impact Level: In most cases, the adverse effect of unauthorized modification to or destruction of product outreach information on overall agency mission functions is expected to be limited. Therefore, the default integrity impact recommended for product outreach information is ***low***.

C.1. 6.3.3 Availability

The effects of disruption of access to or use of product outreach information can usually be repaired. The time frame required for repair is dependent on implementation and use of procedures and controls. Product outreach processes are generally tolerant of limited delays. Mitigating procedures and controls can usually prevent long term or permanent damage to mission capability. In most cases, disruption of access to or use of product outreach information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for product outreach information is ***low***.

C.1.6.4 Public Relations Information Type

Public Relations activities involve the efforts to promote an organizations image through the effective handling of citizen concerns. The recommended security categorization for the public relations information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1. 6.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of public relations information on the ability of responsible agencies to promote an organizations image through the effective handling of citizen concerns. Public relations information itself is almost always in the public domain and poses no confidentiality impact.

Special Factors Affecting Confidentiality Impact Determination: Internal correspondence associated with development of public relations information can contain information, the unauthorized disclosure of which can have a serious adverse effect on agency operations. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for public relations information is ***low***.

C.1. 6.4.2 Integrity

Public relations activities are not usually time-critical. The consequences of unauthorized modification of public relations information can generally be overcome if review procedures are in place and basic procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material. In most cases, the adverse effects of unauthorized modification to or destruction of public relations information on overall agency mission functions should be limited.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of public relations information that is not immediately detected can result in distribution of false and misleading information. Such events can be expected to adversely affect operations and/or public confidence in the agency. This can significantly degrade the public relations mission capability. In such cases, a ***moderate*** integrity impact may exist.

Recommended Integrity Impact Level: The default integrity impact level recommended for public relations information is ***low***.

C.1.6.4.3 Availability

The effects of disruption of access to or use of public relations information can usually be repaired. The time frame required for repair is dependent on implementation and use of basic procedures and controls. Public relations processes are generally tolerant of limited delays. Use of basic procedures and controls can usually prevent long term or permanent damage to mission capability. In most cases, disruption of access to or use of public relations information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for public relations information is ***low***.

C.1.7 Legislative Relations

Legislative Relations involves activities aimed at the development, tracking, and amendment of public laws through the legislative branch of the Federal Government.

C.1.7.1 Legislation Tracking Information Type

Legislation Tracking involves following legislation from conception to adoption. The recommended security categorization for the legislation tracking information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1.7.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of legislation tracking information on the ability of responsible agencies to follow legislation from conception to adoption. Legislation tracking information itself should almost always be in the public domain and pose no confidentiality impact.

Special Factors Affecting Confidentiality Impact Determination: In some cases, internal correspondence associated with legislation tracking information can contain information, the unauthorized disclosure of which can have a serious adverse effect on agency relationships with other agencies and with the legislative branch. This can result in assignment of a ***moderate*** impact level to such information.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for legislation tracking information is ***low***.

C.1.7.1.2 Integrity

Legislation tracking activities are not usually time-critical. The consequences of unauthorized modification of legislation tracking information can generally be overcome if review procedures are in place and basic procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material. In most cases, the adverse effects of unauthorized modification to or destruction of legislation tracking information on overall agency mission functions is expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for legislation tracking information is ***low***.

C.1.7.1.3 Availability

The effects of disruption of access to or use of legislation tracking information can usually be repaired. The time frame required for repair is dependent on implementation and use of basic procedures and controls. Legislation tracking processes are generally tolerant of limited delays. Basic mitigating procedures and controls can usually prevent long term or permanent damage to mission capability. In most cases, disruption of access to or use of legislation tracking information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for legislation tracking information is ***low***.

C.1.7.2 Legislation Testimony Information Type

Legislation Testimony involves activities associated with providing testimony/evidence in support or, or opposition to, legislation from conception to adoption. Subject to exception conditions described below, the recommended security categorization for the legislation testimony information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1.7.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of legislation testimony information on the ability of responsible agencies to provide testimony/evidence in support or, or opposition to, legislation from conception to adoption. Most testimony regarding legislation is in the public domain, and even premature release should result in no more than limited harm to agency assets, personnel, or operations.

Special Factors Affecting Confidentiality Impact Determination: The effects of loss of confidentiality of some information on the basis of which testimony is developed or of early drafts of testimony can result in attempts by competing interests to influence and/or impede a specific legislative process. The consequences to agency programs and even of the ability of an agency to perform its mission can be very serious. Premature public release of draft testimony before internal coordination and review has been conducted can result in unnecessary criticism of the proposed testimony and even damage public confidence in the agency. These consequences are particularly likely where the release includes unedited internal commentary and discussion. The results of unauthorized disclosure of information to the public can imperil specific agency programs, but a consequent loss of public confidence can do persistent harm to an agency's ability to effectively perform its mission. Some information associated with legislative testimony by representatives of some Federal agencies is classified *national security information*. Such information, while extremely sensitive is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for legislation testimony information is ***low***.

C.1.7.2.2 Integrity

The consequences of unauthorized modification or destruction of legislation testimony information can generally be overcome if even minimal mitigating procedures and controls are in use. In most cases, competent agency personnel (e.g., authors and reviewers) should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external publication of testimony associated with legislation (e.g., web pages, electronic mail) may adversely affect inter-agency relationships, relations with

Congress, or public confidence in the agency. However, damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: In general, assuming the implementation and use of basic procedures and controls, the default integrity level recommended for legislation testimony information is ***low***.

C.1.7.2.3 Availability

The effects of disruption of access to or use of legislation testimony information or information systems can usually be repaired. The time frame required for repair is dependent on procedures and controls, but the nature of legislation testimony processes is usually tolerant of delays. Alternate communications media and retention of copies of source material can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Special Factors Affecting Availability Impact Determination: Excessive recovery delays can result in damage to agency reputation and to interests associated with specific legislation.

Recommended Availability Impact Level: The default availability impact level recommended for legislation testimony information is ***low***.

C.1.7.3 Proposal Development Information Type

Proposal Development involves drafting proposed legislation that creates or amends laws subject to Congressional legislative action. Subject to exception conditions described below, the recommended security categorization for the proposal development information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

C.1.7.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of proposal development information on the ability of responsible agencies to draft proposed legislation that creates or amends laws subject to Congressional legislative action. The effects of loss of confidentiality of information on the basis of which proposed legislation is developed or of early drafts of proposed legislation can result in attempts by competing interests to influence and/or impede a specific legislative process. The consequences to agency programs and even of the ability of an agency to perform its mission can be very serious. Premature public release of proposed legislation before internal coordination and review has been conducted can result in unnecessary criticism of the proposed legislation and even damage public confidence in the agency. These consequences are particularly likely where the release includes unedited internal commentary and discussion. In general, unauthorized disclosure of much legislative proposal information, particularly in early phases of the process, is likely to result in serious harm to agency assets or operations.

Special Factors Affecting Confidentiality Impact Determination: Note that some information associated with proposal development by representatives of some Federal agencies (e.g.,

homeland security, law enforcement, defense, intelligence community) is very sensitive or even classified *national security information*. *National security information*, while extremely sensitive is outside the scope of this guideline. The sensitivity level associated with some of the other information is ***high***.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for proposal development information is ***moderate***.

C.1.7.3.2 Integrity

The consequences of unauthorized modification or destruction of proposal development information can generally be overcome if even minimal procedures and controls are implemented and used. In most cases, competent agency personnel (e.g., authors and reviewers) should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external publication of proposed legislation (e.g., web pages, electronic mail) may adversely affect inter-agency relationships, relations with Congress, or public confidence in the agency. However, damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: In general, assuming the implementation and use of basic procedures and controls, the default integrity level recommended for proposal development information is ***low***.

C.1.7.3.3 Availability

The effects of disruption of access to or use of proposal development information or information systems can usually be repaired. The time frame required for repair is dependent on procedures and controls, but the nature of proposal development processes is usually tolerant of delays. Alternate communications media and retention of copies of source material can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Special Factors Affecting Availability Impact Determination: Excessive recovery delays can result in damage to agency reputation and to interests associated with specific legislation.

Recommended Availability Impact Level: In general, the default availability impact level recommended for proposal development information is ***low***.

C.1.7.4 Congressional Liaison Information Type

Congressional Liaison Operations involves all activities associated with supporting the formal relationship between a Federal Agency and the U.S. Congress. Subject to exception conditions described below, the recommended security categorization for the Congressional liaison information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

C.1.7.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of Congressional liaison information on the ability of responsible agencies to support their formal relationships with U.S. Congress. The effects of loss of confidentiality of information associated with Congressional liaison can facilitate attempts by competing interests to influence and/or impede a specific legislative process or poison inter-branch relations. The consequences to agency programs and even of the ability of an agency to perform its mission can be very serious. Premature public release of information associated with Congressional liaison before internal coordination and review has been conducted can result in unnecessary criticism of the preliminary data or positions, and even damage public confidence in the agency. These consequences are particularly likely where the release includes unedited internal commentary and discussion. In general, unauthorized disclosure of much Congressional liaison information is likely to result in serious harm to agency assets and/or operations.

Special Factors Affecting Confidentiality Impact Determination: Note that some information associated with Congressional liaison by representatives of some Federal agencies (e.g., homeland security, law enforcement, defense, intelligence community) is very sensitive or even classified *national security information*. *National security information*, while extremely sensitive is outside the scope of this guideline. The sensitivity level associated with some of the other information is ***high***.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for Congressional liaison information is ***moderate***.

C.1.7.4.2 Integrity

The consequences of unauthorized modification or destruction of Congressional liaison information can generally be overcome if even minimal procedures and controls are implemented and used. In most cases, competent agency personnel (e.g., authors and reviewers) should be able to recognize anomalous information and compare suspect information to that contained in source material. Misunderstandings resulting from modified information that is actually exchanged can usually be resolved. Any resulting damage to the liaison function would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: Assuming the implementation and use of basic procedures and controls, the default integrity level recommended for Congressional liaison information is ***low***.

C.1.7.4.3 Availability

The effects of disruption of access to or use of Congressional liaison information or information systems can usually be repaired. The time frame required for repair is dependent on procedures and controls, but the nature of Congressional liaison processes is usually tolerant of delays. Availability of mitigating procedures and controls, such as alternate communications media and retention of copies of source material, can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Special Factors Affecting Availability Impact Determination: Excessive recovery delays can result in damage to agency reputation and to interests associated with specific legislation.

Recommended Availability Impact Level: The default availability impact level associated with Congressional liaison information is ***low***.

C.1.8 General Government

General Government involves the general overhead costs of the Federal Government, including legislative and executive activities; provision of central fiscal, personnel, and property activities; and the provision of services that cannot reasonably be classified in any other service support area. As a normal rule, all activities reasonably or closely associated with other service support areas or information types shall be included in those service support areas or information types rather than listed as a part of general government. This service support area is reserved for central government management operations; most agency-specific management activities would not be included here. Note also, however, that unlike the other service support functions, some general government information types are associated with specific organizations (e.g., Department of the Treasury, Executive Office of the President, Internal Revenue Service).

C.1.8.1 Central Fiscal Operations Information Type

Central Fiscal Operations includes the fiscal operations that the Department of Treasury performs on behalf of the Government. Note: Tax-related functions are associated with the Taxation Management information type. Note that impacts to some information and information systems associated with central fiscal operations may affect the security of the critical banking and finance infrastructure. In most cases, the effect on public welfare of a loss of central fiscal operations functionality can be expected to be delayed rather than immediate. The potential for consequent loss of human life or of major national assets is relatively low, since the most catastrophic consequences of impairment to mission capability can, in most cases, be corrected before they are fully realized. The default security categorization recommended for the central fiscal operations information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

C.1.8.1 .1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of central fiscal operations information on the fiscal operations that the Department of Treasury performs on behalf of the Government. The effects of loss of confidentiality can reasonably be expected to jeopardize relationships and administrative actions necessary to mission fulfillment and/or to seriously damage public confidence in the agency. For example, the unauthorized disclosure of investigative and enforcement information can have serious economic impact on both individual companies and the broader market place (e.g., short-term stock market perturbations). The consequences of such unauthorized disclosures may have a serious adverse effect on public confidence in the agency.

Special Factors Affecting Confidentiality Impact Determination: Where the operations in question involve liaison with law enforcement or homeland security organizations, the consequences of unauthorized disclosure can imperil operations critical to the security of human

life, critical infrastructure protection, ore the protection of key national assets. For those operations on a macroeconomic scale, the consequences to key financial infrastructure elements can be serious to severe. In such cases, the associated confidentiality impact level would be ***moderate*** to ***high***.

Recommended Confidentiality Impact Level: The confidentiality impact level recommended for most central fiscal operations information is ***moderate***.

C.8.1.1.2 Integrity

The consequences of unauthorized modification or destruction of central fiscal operations information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that include central fiscal operations information (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: Assuming the implementation and use of basic procedures and controls, the integrity impact level associated with central fiscal operations information is normally ***low***.

C.8.1.1.3 Availability

The effects of disruption of access to or use of central fiscal operations information or information systems can usually be repaired. The time frame required for repair is dependent on implementation and use of basic procedures and controls, but the nature of central fiscal operations processes is usually tolerant of delays. Mitigating procedures and controls like having alternate communications media and retention of copies of source material can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Recommended Availability Impact Level: Assuming the implementation and use of basic procedures and controls, the availability impact level associated with central fiscal operations information is normally ***low***.

C.1.8.2 Legislative Functions Information Type

Legislative functions include the service support activities associated with costs of the Legislative Branch other than the Tax Court, the Library of Congress, and the Government Printing Office revolving fund. The recommended security categorization for the legislative service support information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1. 8.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of legislative service support information on the ability of responsible agencies to provide service support activities associated with costs of the Legislative Branch other than the Tax Court, the Library of Congress, and the Government Printing Office revolving fund. The effects of loss of confidentiality of information associated with legislative service support can generally be expected to have only a limited impact on Federal government assets, operations, or personnel welfare.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for legislative service support information is ***low***.

C.1.8.2.2 Integrity

The consequences of unauthorized modification or destruction of legislative service support information can generally be overcome if even minimal procedures and controls are implemented and used. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material. Misunderstandings resulting from modified information that is actually exchanged can usually be resolved. Any resulting damage to the support function would usually be limited and can generally be corrected within reasonable time and resource constraints.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external publication of legislative service support information (e.g., web pages, electronic mail) may adversely affect inter-agency relationships, relations with Congress, or public confidence in the agency. However, damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: Assuming the implementation and use of basic procedures and controls, the default integrity level recommended for legislative service support information is ***low***.

C.1.8.2.3 Availability

The effects of disruption of access to or use of legislative service support information or information systems can usually be repaired. The time frame required for repair is dependent on procedures and controls, but the nature of legislative service support processes is usually tolerant of delays. Mitigating procedures and controls like having alternate communications media and retention of copies of source material can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Special Factors Affecting Availability Impact Determination: Excessive recovery delays can result in damage to agency reputation and to interests associated with specific legislation.

Recommended Availability Impact Level: The availability impact level recommended for most legislative service support information is ***low***.

C.1.8.3 Executive Functions Information Type

Executive Functions involve the Executive Office of the President. Subject to exception conditions described below, the recommended security categorization for the executive information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, MODERATE), (**availability**, HIGH)}

C.1.8.3.1 Confidentiality

The confidentiality impact level associated with the executive information type is associated with functions of the Executive Office of the President. The effects of loss of confidentiality of policies and guidance during the formative stage can result in attempts by affected entities and other interested parties to influence and/or impede the policy and guidance development process. Premature public release of formative policies and guidance before internal coordination and review can result in unnecessary damage to public confidence in the Executive Office of the President. This is particularly likely where the release includes unedited internal commentary and discussion. These consequences are particularly likely where the release includes unedited internal commentary and discussion.

Special Factors Affecting Confidentiality Impact Determination: Note that much information processed in and by the Executive Office of the President is classified *national security information*. Such information, while extremely sensitive is outside the scope of this guideline. Other information processed in and by the Executive Office of the President (EOP) involves extremely sensitive homeland security, law enforcement, and other information, the unauthorized disclosure of which can seriously imperil human life, key national assets, and critical infrastructures.

Recommended Confidentiality Impact Level: Based on the catastrophic harm that can be suffered by the nation due to unauthorized disclosure of executive information (and associated commentary), the default confidentiality impact level recommended for executive information is ***high***.

C.1.8.3.2 Integrity

The consequences of unauthorized modification or destruction of executive information can generally be overcome if basic procedures and controls are implemented and used. In most cases, competent EOP personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Recommended Integrity Impact Level: Unauthorized modification or destruction of information affecting external communications that contain EOP information (e.g., web pages, electronic mail) may adversely affect public confidence in the government. In the case of the EOP, the impact of such a loss of public confidence may be at least ***moderate***.

Recommended Integrity Impact Level: The default integrity impact level recommended for executive information is ***moderate***.

C.1.8.3.3 Availability

The effects of disruption of access to or use of executive information or information systems can usually be repaired. The time frame required for repair is dependent on procedures and controls, but the nature of national defense and critical infrastructure protection aspects of EOP functions is not reliably tolerant of delays. Excessive recovery delays can result in loss of coordination of critical defense and public welfare processes.

Recommended Availability Impact Level: The default availability impact level recommended for executive information is ***high***.

C.1.8.4 Central Property Management Information Type

Central Property Management involves most of the operations of the General Services Administration. The following recommended default security categorization of central property management information is particularly subject to change where critical infrastructure elements or key national assets are involved:

SECURITY CATEGORY = {(**confidentiality**, LOW[3]), (**integrity**, LOW[10]), (**availability**, LOW[4])}

C.1.8.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of central property management information on the ability of the General Services Administration to acquire, provide, and centrally administer offices buildings, fleets, machinery, and other capital assets and consumable supplies used by the Federal government. The consequences of unauthorized disclosure of most central property management information are likely to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of information associated with very large procurements can result in fraud, waste, abuse, and/or legal proceedings that can have a serious to severe effect on Federal government assets and operations. Also, information associated with acquisition, maintenance, administration, and operation of many Federal government office buildings, transportation fleets, and operational facilities can be of material use to criminals seeking to gain access to Federal facilities in order to facilitate or perpetrate fraud, theft, or some other criminal enterprise. In this case, unauthorized disclosure of information can have a serious adverse effect on agency operations, agency assets, or individuals. The consequent confidentiality impact would be at least ***moderate.*** Information associated with maintenance, administration, and operation of other Federal government facilities can be of material use to terrorists seeking to penetrate and/or commandeer such facilities as part of operations intended to harm critical infrastructures, key national assets, or people. Examples of such more potentially damaging information include architectural, maintenance and administrative information that might permit either covert pedestrian or unimpeded vehicular access to government buildings (e.g., Congressional office buildings, FBI Headquarters, the National Archives, Smithsonian Institution buildings, dams, nuclear power

[3] Impact level is usually ***high*** where safety of major critical infrastructure components or key national assets is at stake.

[4] Impact level is usually ***moderate*** to ***high*** in emergency situations where time-critical processes affecting human safety or major assets are involved.

plants, etc.). In such cases, the confidentiality impact must be considered to be ***high***. [Note that some GSA information is classified. The classified information is *national security related* and is outside the scope of this guideline.] Also, either anticipated or realized unauthorized disclosure of one agency's central property management information by GSA could result in negative impacts on cross-jurisdictional coordination within the central property management infrastructure and the general effectiveness of organizations tasked with acquisition, provision, and management of government facilities and supplies.

Recommended Confidentiality Impact Level: The confidentiality impact level recommended for most central property management information is ***low***.

C.1.8.4.2 Integrity

The consequences of unauthorized modification to or destruction of central property management information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately. The consequences of unauthorized modification to or destruction of central property management information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external publication of central property management information (e.g., web pages, electronic mail) may adversely affect public confidence in the agency. However, damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most central property management information is ***low***.

C.1.8.4.3 Availability

The effects of disruption of access to or use of central property management information or information systems can usually be expected to be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on procedures and controls, but the nature of functions supported by most central property management information is tolerant of delays.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency response aspects of disaster management. In such cases, delays measured in hours can cost lives and major property damage. Consequently, the availability impact level associated with unauthorized modification or destruction of central property management information needed to respond to emergencies can be ***high***. The more common case is likely to be that disruption of access has a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: In general, given implementation and use of basic procedures and controls and where processes to which the information is essential are either not

time-critical or not likely to have serious or severe consequences, the availability impact level recommended for central property management information is ***low***.

C.1.8.5 Central Personnel Management Information Type

Central Personnel Management involves most of the operating activities of the Office of Personnel Management and related agencies. The recommended security categorization for the central personnel management information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.1.8.5.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of central personnel management information on the ability of the Office of Personnel Management (OPM) to build a high quality and diverse Federal workforce, based on merit system principles. Central personnel management information includes human resources management and consulting services, education and leadership development services, and investigation services. It is anticipated that unauthorized disclosure of most central personnel management information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974 or other laws and executive orders. Such information will often be assigned a ***moderate*** confidentiality impact level. Some information associated with investigative services may be particularly sensitive.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for central personnel management information is ***low***.

C.1.8.5.2 Integrity

The consequences of undetected unauthorized modification or destruction of central personnel management information can conceivably disrupt central personnel management operations (e.g., (e.g., by modifying sensitive private personal information or compromising confidentiality mechanisms). However, given availability and use of basic procedures and controls, agency personnel can usually be expected to recognize anomalous information and compare suspect information to that contained in original sources. The damage likely to be caused by unauthorized modification or destruction of central personnel management information is likely to be detected and corrected before it adversely affects government operations or public confidence in the government.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external publication of central personnel management information (e.g., web pages, electronic mail) may adversely affect public confidence in the government. However, damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for central personnel management information is ***low***.

C.1.8.5.3 Availability

The effects of disruption of access to or use of central personnel management information can usually be repaired. The time frame required for repair is dependent on implementation and use of basic procedures and controls. Central personnel management processes are generally tolerant of reasonable delays. Mitigating procedures and controls like availability and use of alternate facilities can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of central personnel management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The base availability impact recommended for central personnel management information is ***low***.

C.1.8.6 Taxation Management Information Type

Taxation Management includes activities associated with the implementation of the Internal Revenue Code and the collection of taxes in the United States and abroad. The recommended security categorization for the taxation management information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

C.1.8.6.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of taxation management information on the ability of the Internal Revenue Service (IRS) to enforce the Internal Revenue Code and to collect taxes in the United States and abroad. Taxpayer information associated with taxation management is regulated by Section 1.16 of the Internal Revenue Manual (IRM), the Privacy Act of 1974, the Economic Espionage Act, the Freedom of Information Act, and the Federal Information Security Management Act. The IRS *Guidebook for Information Sensitivity Analysis* provides guidelines for identifying IRS Official Use Only (OUO) Information. Sensitive information is identified in the IRM as any information which if lost, stolen, (accessed), or altered without proper authorization may adversely affect Service operations. The IRM states that unauthorized disclosure of sensitive information may cause lawsuits against Service officials as well as the Service, unwanted notoriety for the Service, and public distrust of the Service's ability to protect such information – all of which may result in an increase in noncompliance with tax laws. It notes that unauthorized release of information such as the name and address of an informant (in cases of tax evasion or fraud) may threaten a person's life.[5] Additionally, sensitive information is defined in Section 25.10 of the IRM as information that requires protection due to the risk or magnitude of loss that could result from inadvertent or deliberate disclosure of the information. Sensitive information includes information whose improper use could adversely affect the ability of the agency to accomplish its mission, proprietary information, records about individuals that require protection under the Privacy Act, and information not releasable under the Freedom of Information Act. The IRS OUO guideline

[5] Such information would have a ***high*** confidentiality default confidentiality impact rating.

notes that prevention of unauthorized disclosure of information revealing internal matters, the disclosure of which would risk circumvention of a legal requirement or agency rules and regulations (often referred to as "high 2" information) has assumed an increasingly important role in homeland security. Unauthorized disclosure of sensitive or private IRS information can be expected to have a serious effect on both the welfare of individuals and public confidence in the government.

Special Factors Affecting Confidentiality Impact Determination: In cases where unauthorized disclosure of taxation information can impede anti-terrorism or other homeland security activities or endanger the lives of agents or informants, the confidentiality impact level is ***high***.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for taxation management information is ***moderate***.

C.1.8.6.2 Integrity

Most taxation management activities are not usually time-critical. Exceptions are taxation management activities associated with law enforcement criminal investigation or homeland security activities. The consequences of unauthorized modification of taxation management information that is not time-critical can generally be overcome if basic procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Special Factors Affecting Integrity Impact Determination: There is a potential for tax code enforcement, other law enforcement, or anti-terrorism actions being taken based on modified or incomplete information. Also, unauthorized modification or destruction of taxation management information that is not immediately detected can result in distribution of false and misleading information. Such events can be expected to adversely affect individuals, operations, and/or public confidence in the agency. This can significantly degrade the taxation management mission capability. In extreme cases (e.g., misidentification of an informant), the consequences can be life threatening. In such cases, a ***high*** integrity impact may exist.

Recommended Integrity Impact Level: Given diligent adherence to at least basic procedures and controls, the adverse effects of unauthorized modification to or destruction of taxation management information on overall agency mission functions is expected to be limited. Therefore, the default integrity impact level recommended for taxation management information is ***low***.

C.1.8.6.3 Availability

The effects of disruption of access to or use of taxation management information can usually be repaired. The time frame required for repair is dependent on implementation and use of basic back up information, facilities and procedures. Taxation management processes are generally tolerant of limited delays. Availability and use of basic mitigating procedures and controls can usually prevent long term or permanent damage to mission capability. However, even temporary loss of availability of taxation management information is likely to have an adverse effect on public confidence in the agency and on Federal government cash flow.

Special Factors Affecting Availability Impact Determination: While most cases will result in only limited consequences, repeated disruptions can have a serious adverse effect on public confidence in the agency. This can significantly degrade the taxation management mission capability (e.g., via reduced taxpayer compliance). In such cases, the availability impact might be ***moderate***. Loss of availability of significant amounts of taxation management information over long periods of time can do serious harm to Federal government operations. The economic ramifications would potentially be severe.

Recommended Availability Impact Level: In most cases, disruption of access to or use of taxation management information can be expected to have only a limited adverse effect on overall agency operations, agency assets, or individuals. Therefore, the default availability impact recommended for taxation management information and information systems is ***low***.

C.1.8.7 Central Records and Statistics Management Information Type

Central Records and Statistics Management involves the operations surrounding the management of official documents, statistics, and records for the entire Federal Government. This information type is intended to include information and information systems associated with the management of records and statistics for the Federal government as a whole, such as the records management performed by NARA or the statistics and data collection performed by the Bureau of the Census. Note: Many agencies perform records and statistics management for a particular business function and as such should be mapped to the service support, management, or mission area associated with that business function. The central records and statistics management information type is intended for functions performed on behalf of the entire Federal government. The recommended security categorization for the central records and statistics management information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

C.1.8.7.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of central records and statistics management information on the ability of responsible agencies to manage official documents, statistics, and records for the entire Federal Government. Unauthorized disclosure of raw data and other source information for central records and statistics management operations is likely to violate the Privacy Act of 1974 and other laws and executive orders regulating dissemination of personal and government information.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some centrally managed records can pose a threat to human life or a loss of major assets. In such cases, the confidentiality impact is ***high***.

Recommended Confidentiality Impact Level: Although there are many cases in which unauthorized disclosure of centrally managed records will have only a limited adverse effect on government operations, assets, or individuals, the default confidentiality impact level recommended for central records and statistics management information is ***moderate***.

C.1.8.7.2 Integrity

Given availability and use of basic procedures and controls, agency personnel can often recognize anomalous information and compare suspect information to that contained in original sources. The damage likely to be caused by unauthorized modification or destruction of central records and statistics management information is likely to be detected and corrected before it adversely affects agency operations or public confidence in the agency.

Recommended Integrity Impact Level: The default integrity impact level assigned to central records and statistics management information is ***low***.

C.1.8.7.3 Availability

The effects of disruption of access to or use of central records and statistics management information can usually be repaired. The time frame required for repair is dependent on implementation and use of at least basic mitigating controls and procedures. Central records and statistics management processes are generally tolerant of reasonable delays. Basic mitigating controls and procedures such as disaster recovery measures can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of central records and statistics management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The base availability impact recommended for central records and statistics management information is ***low***.

C.2 Government Resource Management Information

Resource management functions are the back office support activities that enable the government to operate effectively. Security objectives and impacts for resource management functions are determined by the direct service missions and constituencies ultimately being supported. It is likely that all Federal government information systems store, process, and operate under the control of information technology (IT) infrastructure maintenance information (e.g., password files and file and network access settings). At least a basic set of security controls will apply to this set of information and processes in order to combat potential corruption, misuse, or abuse of system information and processes.

C.2.1 Administrative Management

Administrative Management involves the day-to-day management and maintenance of the internal infrastructure. Administrative information is, by its nature, usually routine and is relatively low impact. However, some administrative management information is either quite sensitive (e.g., logistics management for nuclear or other hazardous materials, security management information, and security clearance management information) or critical (e.g., inventory control and logistics management information needed to support time-critical operations). Note that any *national security information* is outside the scope of this guideline. [See Appendix A, Glossary of Terms, for a definition of *national security information/systems.*] Routine administrative management information systems that do not process classified information are not usually designated *national security systems*, even if they are critical to the direct fulfillment of military or intelligence missions.[13]

C.2.1.1 Facilities, Fleet, and Equipment Management Information Type

Facilities, Fleet, and Equipment management involves the maintenance, administration, and operation of offices buildings, fleets, machinery, and other capital assets considered as possessions of the Federal government. Note that impacts to some information and information systems associated with facilities, fleet, and equipment management may inherently affect the security of some key national assets (e.g., nuclear power plants, dams, and other government facilities). The following recommended default categorization of the facilities, fleet, and equipment management information type is particularly subject to change where critical infrastructure elements or key national assets are involved:

SECURITY CATEGORY = {(**confidentiality**, LOW[6]), (**integrity**, LOW[10]), (**availability**, LOW[7])}

C.2.1.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of facilities, fleet, and equipment management information on the ability of responsible agencies to maintain, administer, and operate offices buildings, fleets, machinery, and other capital assets of the Federal government. The consequences of unauthorized disclosure of most facilities, fleet, and equipment management information are likely to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Information associated with maintenance, administration, and operation of many Federal government office buildings, transportation fleets, and operational facilities can be of material use to criminals seeking to gain access to Federal facilities in order to facilitate or perpetrate fraud, theft, or some other criminal enterprise (e.g., extract inmates from Federal detention facilities). In this case, unauthorized disclosure of information can have a serious adverse effect on agency operations, agency assets, or individuals. The consequent confidentiality impact would be at least ***moderate.*** Information associated with maintenance, administration, and operation of other Federal government office buildings, transportation fleets, and operational facilities can be of material use to terrorists seeking to penetrate and/or commandeer such facilities as part of operations intended to harm critical infrastructures, key national assets, or people. Examples of such more potentially damaging information includes information that reveals specific measures respecting limiting access to and operation of government aircraft, maintenance and administrative information that might permit either covert pedestrian or unimpeded vehicular access to government buildings (e.g., Congressional office buildings, FBI Headquarters, the National Archives, Smithsonian Institution buildings, dams, nuclear power plants, etc.), and schedules/itineraries of government surface transportation fleets (e.g., for transport of executive personnel or hazardous materials). In these cases, the confidentiality impact must be considered to be ***high***. [Note that some information regarding transportation and storage of nuclear materials is classified. The classified information is *national security related* and is outside the scope of this guideline. Other information, such as Nuclear Regulatory Commission "SAFEGUARDS" information is not *national security information*, but must be treated as having ***high*** confidentiality impact.] Also,

[6] Impact level is usually ***high*** where safety of major critical infrastructure components or key national assets are at stake.

[7] Impact level is usually ***moderate*** to ***high*** in emergency situations where time-critical processes affecting human safety or major assets are involved.

either anticipated or realized unauthorized disclosure of one agency's facilities, fleet, and equipment management information by another agency could result in negative impacts on cross-jurisdictional coordination within the facilities, fleet, and equipment management infrastructure and the general effectiveness of organizations tasked with facilities, fleet, and/or equipment management.

Recommended Confidentiality Impact Level: In spite of the aforementioned cases where there is ***moderate*** or ***high*** impact associated with unauthorized disclosure of facilities, fleet, and equipment management information, the confidentiality impact level recommended for most facilities, fleet, and equipment management information is ***low***.

C.2.1.1.2 Integrity

The consequences of unauthorized modification to or destruction of facilities, fleet, and equipment management information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately.

Special Factors Affecting Integrity Impact Determination: Exceptions may include emergency response aspects of disaster management or leadership protection. In such cases, the integrity impact level associated with unauthorized modification or destruction of facilities, fleet, and equipment management information can be ***high***. The consequences of unauthorized modification to or destruction of less time-critical facilities, fleet, and equipment management information can generally be overcome if back-up and archiving procedures are basic and are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most facilities, fleet, and equipment management information is ***low***.

C.2.1.1.3 Availability

The effects of disruption of access to or use of facilities, fleet, and equipment management information or information systems can usually be expected to be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of functions supported by most facilities, fleet, and equipment management information is tolerant of delays.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency response aspects of disaster management or leadership protection. In such cases, delays measured in seconds can cost lives and major property damage. Consequently, the availability impact level associated with unauthorized modification or destruction of facilities, fleet, and equipment management information needed to respond to emergencies can be ***high***. The more common case is likely to be that disruption of access has a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: In general, given implementation and use of basic procedures and controls, where processes to which the information is essential are either not time-critical or not likely to have serious or severe consequences, the default availability impact level recommended for facilities, fleet, and equipment management information is ***low***.

C.2.1.2 Help Desk Services Information Type

Help Desk Services involves the management of a service center to respond to government employees' technical and administrative questions. Subject to exception conditions described below, the recommended default security categorization for the help desk service information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.1.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of help desk service information on the ability of responsible agencies to manage of service center responses to government employees' technical and administrative questions. The consequences of unauthorized disclosure of most help desk service information are likely to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Information associated with service center responses can provide useful information to adversaries seeking to penetrate Federal systems. If the contents or functions of a system have sufficient sensitivity and/or criticality, a higher impact level may be considered for help desk information.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for help desk service information is ***low***.

C.2.1.2.2 Integrity

The consequences of unauthorized modification to or destruction of help desk service information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately. In relatively few cases would the consequences of unauthorized modification of help desk information that is acted upon immediately result in more than limited damage to agency operations or assets.

Special Factors Affecting Integrity Impact Determination: Exceptions may include bogus information regarding operation of communications processors, data base systems, or other systems necessary to emergency response aspects of disaster management, criminal apprehension, air traffic control or other time-critical missions. In such cases, a ***moderate*** or ***high*** integrity impact level might be considered for unauthorized modification or destruction of help desk service information.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of help desk service information is ***low***.

C.2.1.2.3 Availability

The effects of disruption of access to or use of help desk service information or information systems can usually be expected to be repaired in time to prevent catastrophic loss.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency response aspects of disaster management or other high load and time critical functions (e.g., some systems that support air traffic control functions). Consequently, the availability impact level associated with unauthorized modification or destruction of help desk service information needed to respond to emergencies can be ***high***. The far more common case is likely to be that disruption of access has a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: In general, where processes to which the information is essential are either not time-critical or not likely to have serious or severe consequences, the default availability impact level recommended for help desk service information is ***low***.

C.2.1.4 Security Management Information Type

Security Management involves the physical protection of an organization's personnel, assets, and facilities. Note that impacts to some information and information systems associated with security management may inherently affect the security of some critical infrastructure elements and key national assets (e.g., nuclear power plants, dams, and other government facilities). Impact levels associated with security information directly relate to the value, criticality, and potential threat to human life associated with the asset(s) being protected by a particular security management instantiation (e.g., consequences to the public of terrorist access to dams or nuclear power plants). The following recommended categorization of the facilities, fleet, and equipment management information type is subject to change where critical infrastructure elements or key national assets are involved:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)}

C.2.1.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of security management information on the ability of responsible organizations to physically protect their personnel, assets, and facilities. The consequences of unauthorized disclosure of most security management information depend on the likelihood that the information might jeopardize the physical security of an organization's assets and the value, and potential for collateral damage, of the assets being protected. The consequences of unauthorized disclosure of information that permits a breach in the physical security of hospital pharmaceutical storage or of storage for an organization's cash assets are likely to have only a limited adverse effect on agency operations, agency assets, or individuals. Such information merits only a ***low*** confidentiality impact.

Special Factors Affecting Confidentiality Impact Determination: Information associated with the physical security of many Federal government office buildings, transportation fleets, and operational facilities can be of material use to criminals seeking to gain access to Federal facilities in order to facilitate or perpetrate a major crime (e.g., extraction of inmates from Federal detention facilities, theft of commodities market projections, access to information

associated with a felony criminal investigation or prosecution, theft of blank license issuing facilities and/or materials, access to competition-sensitive information associated with major procurements, undetected access to national archives or museum properties, access to currency printing facilities or materials, theft of major currency or bullion storage facilities). In such cases, unauthorized disclosure if information can have a serious adverse effect on agency operations, agency assets, or individuals. The consequent confidentiality impact would be at least ***moderate.*** Information associated with security management at other Federal government office buildings, transportation fleets, and operational facilities can be of material use to terrorists seeking to penetrate and/or commandeer such facilities as part of operations intended to harm critical infrastructures, key national assets, or people. Examples of such more potentially damaging information includes information that reveals specific measures respecting physical protection of government aircraft, information that might permit either covert pedestrian or unimpeded vehicular access that creates an opportunity to bomb a government building (e.g., Congressional office buildings, FBI Headquarters, the National Archives, Smithsonian Institution buildings, dams, nuclear power plants, etc.), and leadership protection details that could lead to assassination opportunities. In these cases, the confidentiality impact must be considered to be ***high***. Unauthorized disclosure of security management information that can be reasonably expected to pose a serious threat to human life (including those of security guards) must also be assigned a ***high*** confidentiality impact. Note that security management information associated with some Federal government assets is classified. The classified information is *national security related* and is outside the scope of this guideline. Other security management information, such as that affecting Nuclear Regulatory Commission "SAFEGUARDS" or Internal Revenue Service "Limited For Official Use Only" information is not *national security information*, but must definitely be treated as having ***high*** confidentiality impact. Also, either anticipated or realized unauthorized disclosure of one agency's security management information by another agency could result in negative impacts on cross-jurisdictional coordination within the security management infrastructure and the general effectiveness of organizations tasked with physical protection of Federal facilities. In spite of the aforementioned cases where there is ***low*** or ***high*** impact associated with unauthorized disclosure of security management information, the consequences of physical protection failures at most Federal facilities are more likely to result in serious[8] adverse effects that limited or catastrophic adverse effects.

Recommended Confidentiality Impact Level: The confidentiality impact level recommended for most security management information is ***moderate.***

C.2.1.4.2 Integrity

The consequences of unauthorized modification to or destruction of security management information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In many cases, it is likely that the information will be acted upon before a modification or deletion is detected.

Special Factors Affecting Integrity Impact Determination: Exceptions may include standing policies and procedures and bogus schedule changes for guards that are likely to be detected as a result of sound management procedures. In many cases such as these, competent agency

[8] A loss of confidentiality that causes a significant degradation in mission capability, places the agency at a significant disadvantage, or results in major damage to assets, requiring extensive corrective actions or repairs.

personnel may be able to recognize anomalous information and compare suspect information to that contained in source material. In such cases, the integrity impact level associated with unauthorized modification or destruction of security management information can be ***low***. The consequences of unauthorized modification to or destruction of more time-critical security management information or information that is likely to be implemented before it is questioned can reasonably be expected to result in physical security vulnerabilities. The range of potential consequences is covered in Section C.2.1.4.1, Confidentiality. There is a sufficient preponderance of this more vulnerable information that it is prudent to assume successful exploitation of unauthorized modification or destruction of security management information by adversaries responsible for the modification or destruction.

Recommended Integrity Impact Level: In view of the potential consequences discussed in Appendix C.2.1.4.1, the default integrity impact level recommended for most security management information is ***moderate***.

C.2.1.4.3 Availability

Given adequate operational procedures and a responsible training regimen, the effects of disruption of access to or use of security management information or information systems can usually be expected to be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of functions supported by most security management information is tolerant of delays.

Special Factors Affecting Availability Impact Determination: Exceptions may include alarm and alert communications inputs to and interconnections for security management systems and automated control systems that support security management processes (e.g., door and gate operations in buildings to which access is limited such as detention facilities and many Federal office buildings and operational facilities. In some cases, delays measured in seconds or minutes can cost lives and major property damage. The availability impact level associated with unauthorized modification or destruction of such alarm, alert, and automated process security management information in can be ***high***. The more common case is likely to be that disruption of access has a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: In general, given basic procedures and controls (e.g., adequate force training for outage contingencies and implementation and use of adequate back up mechanisms and procedures), and where processes to which the information is essential are either not time-critical or not likely to have serious or severe consequences, the default availability impact level recommended for security management information is ***low***.

C.2.1.5 Travel Information Type

Travel involves the activities associated with planning, preparing, and monitoring of business related travel for an organization's employees. The following security categorization is recommended for the travel information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.1.5.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of travel information on the abilities of responsible agencies to plan, prepare, and monitor business related travel for the organization's employees.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of employee identification information coupled with credit information (e.g., name, social security number, credit card number) can result in moderate to serious consequences for individuals and local organizations. In such cases, the potential for serious adverse effects, especially for individuals and with respect to Privacy Act Information, may justify a ***moderate*** impact level. Also, unauthorized disclosure of information concerning carrier/provider contract negotiations can conceivably have significant financial or legal consequences and put an agency at a serious disadvantage. More severe consequences may stem from unauthorized disclosure of information regarding leadership travel plans or travel associated with classified or otherwise identity and itinerary-sensitive information that might reasonably be expected to jeopardize VIP security or the confidentiality of sensitive operations plans. In the most sensitive cases, the confidentiality impact incurred can be ***high***. However, generally, the consequences of unauthorized disclosure of the vast majority of travel information will result in, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for travel information is ***low***.

C.2.1.5.2 Integrity

The consequences of unauthorized modification to or destruction of travel information depends, not only on mitigating procedures and controls, but on the urgency with which the information is normally needed and the consequences of aborted or disadvantageously modified travel. In the case of travel records maintained for accounting purposes, the consequences of unauthorized modification or destruction of travel information can usually be overcome if basic procedures and controls are adequate and are implemented. In many cases, competent agency personnel should be able to recognize anomalous information (e.g., by comparing suspect information to that contained in source material, back-up files, and/or archives).

Special Factors Affecting Integrity Impact Determination: In the case of travel planning information, there is a higher probability that an integrity compromise will not be noticed before its consequences are felt, but the effects of such modifications are generally limited with respect to agency mission capabilities or assets. Any resulting damage can generally be corrected within reasonable time and resource constraints. It is possible to postulate scenarios in which integrity compromise of travel information may expose Federal leadership to harm or endanger a sensitive or critical operation. However, most such scenarios are dealt with in the context of impacts to mission operations information (Appendix D).

Recommended Integrity Impact Level: The default integrity impact level recommended for travel information is ***low***.

C.2.1.5.3 Availability

The effects of disruption of access to or use of travel information or information systems can usually be repaired within reasonable time and resource constraints. The time frame required for repair is dependent implementation and use mitigating procedures and controls. The nature of travel processes is usually tolerant of reasonable delays, at least on the "agency mission" scale. In the case of travel accounting activities, the disruption of access to travel information can usually be overcome if basic procedures and controls are implemented. (E.g., use of alternate communications and processing facilities and retention of copies of travel-related transaction records can generally facilitate recovery and prevent major compromise of mission capability).

Recommended Availability Impact Level: The default availability impact level recommended for travel information is normally ***low***.

C.2.1.6 Workplace Policy Development and Management Information Type (*Intra-Agency Only*)

Workplace policy development and management includes all activities required to develop and disseminate workplace policies such as dress codes, time reporting requirements, telecommuting, etc. The following security categorization is recommended for the workplace policy development and management information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.1.5.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of workplace policy development and management information on the abilities of responsible agencies to develop and disseminate workplace policies such as dress codes, time reporting requirements, and telecommuting. The consequences of unauthorized disclosure of the vast majority of workplace policy development and management information will result in, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for workplace policy development and management information is ***low***.

C.2.1.5.2 Integrity

The consequences of unauthorized modification to or destruction of workplace policy development and management information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. Also, in the case of workplace policy development and management planning information, there is a high probability that an integrity compromise will be noticed before its consequences are felt. In any case, the effects of modifications to or deletion of this information are generally limited with respect to agency mission capabilities or assets. Any resulting damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for workplace policy development and management information is ***low***.

C.2.1.5.3 Availability

The effects of disruption of access to or use of workplace policy development and management information or information systems can usually be repaired within reasonable time and resource constraints. The time frame required for repair is dependent on mitigating procedures and controls. The nature of workplace policy development and management processes is tolerant of reasonable delays. In the case of workplace policy development and management records, the disruption of access to records can usually be overcome if basic procedures and controls are implemented.

Recommended Availability Impact Level: The default availability impact level recommended for workplace policy development and management information is ***low***.

C.2.2 Financial Management

Financial management involves the aggregate set of accounting practices and procedures that allow for the accurate, efficient, transparent, and effective handling of all government revenues, funding, and expenditures. Confidentiality impacts associated with financial management information are generally associated with the sensitivity of the existence of specific projects, programs, and/or technologies that might be revealed by unauthorized disclosure of information. Integrity impacts can usually be mitigated through financial audit procedures, but even temporarily successful frauds can affect agency image, and corrective actions are often disruptive to agency operations. Permanent loss/unavailability of financial management information can cripple agency operations. However, back-up/archiving mechanisms and procedures can usually prevent such catastrophic loss.

C.2.2.1 Cost Management Information Type

Assets and Liability Management provide accounting support for the management of assets and liabilities of the Federal government. Assets and liability management activities measure the total cost and revenue of Federal programs, and their various elements, activities and outputs. Assets and liability management is essential for providing accurate program measurement information, performance measures, and financial statements with verifiable reporting of the cost of activities. The recommended security categorization for the assets and liability management information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.2.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of assets and liability management information on the ability of responsible agencies to provide accounting support for the management of assets and liabilities of the Federal government.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some assets and liability management information for programs that process classified or high-impact information can assist some more sophisticated criminals to evade enforcement activities. Examples range from the encouragement of tax evasion that can result from unauthorized disclosure of very detailed information regarding audit budgets for tax collection activities to disclosure of vulnerabilities that unauthorized disclosure of budget details for specific border

control, antiterrorism, or witness protection expenditures can provide to the more sophisticated criminal or terrorist organizations. Where actions taken based on unauthorized disclosure of assets and liability management details can pose a threat to human life or a loss of major assets, the confidentiality impact is ***high***. However, in the vast majority of cases, unauthorized disclosure of assets and liability management information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The recommended default confidentiality impact level for assets and liability management information is ***low***.

C.2.2.1.2 Integrity

The accuracy of assets and liability management information is essential to providing accurate program measurement information, performance measures, and financial statements with verifiable reporting of the cost of activities. The consequences of unauthorized modification to or destruction of assets and liability management information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. Assets and liability management activities are not generally time-critical. The consequences of unauthorized modification or assets and liability management information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency audit personnel should be able to recognize grossly anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives.

Special Factors Affecting Integrity Impact Determination: If reports based on modified or incomplete information are circulated, the adverse effect on mission functions and public confidence in the agency can be serious. In such cases, the integrity impact would be ***moderate***. However, more common case would be only limited adverse effects on agency operations, agency assets, or individuals.

Recommended Integrity Impact Level: The default integrity impact level recommended for most assets and liability management information is ***low***.

C.2.2.1.3 Availability

The effects of disruption of access to or use of assets and liability management information can usually be repaired. The time frame required for repair is dependent on implementation and use of mitigating procedures and controls. Assets and liability management processes are generally tolerant of delay. Availability and use of basic procedures and controls can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of assets and liability management information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for assets and liability management information is ***low***.

C.2.2.2 Reporting and Information Information Type

Reporting and Information includes providing financial information, reporting and analysis of financial transactions. Financial reporting includes the activities necessary to support:

management's fiduciary role; budget formulation and execution functions; fiscal management of program delivery and program decision making; and internal and external reporting requirements. The recommended security categorization for the "financial reporting and information" information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

C.2.2.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of financial reporting information on an agency's ability to provide financial information, reporting and analysis of financial transactions. Unauthorized disclosure of financial reporting information for programs that process classified or high-impact information can give adversaries damaging insights into details of agency plans, priorities, and operations.

Special Factors Affecting Confidentiality Impact Determination: In relatively rare cases, actions taken based on unauthorized disclosure of financial reporting details can pose a threat to human life or a loss of major assets, so the confidentiality impact is ***high***. However, in most cases, unauthorized disclosure of financial reporting information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for financial reporting information is ***low***.

C.2.2.2.2 Integrity

Financial reporting activities are not generally time-critical. The consequences of unauthorized modification or financial reporting information can generally be overcome if mitigating procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize grossly anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives.

Special Factors Affecting Integrity Impact Determination: If planning documents, proposals, or reports based on modified or incomplete information are circulated, the adverse effect on mission functions or public confidence in the agency can be serious. In most cases, serious adverse effects on agency operations, agency assets, or individuals can be expected. The extensive audit and investigative actions that often follow discovery of an agency's use of falsified financial reports or omission of financial reporting data can place the agency at a significant disadvantage and require extensive corrective actions. However, the more common case would be only limited adverse effects on agency operations, agency assets, or individuals.

Recommended Integrity Impact Level: The default integrity impact level recommended for most financial reporting information is ***moderate***.

C.2.2.2.3 Availability

The effects of disruption of access to or use of financial reporting information can usually be repaired. The time frame required for repair is dependent on implementation and use of basic procedures and controls. Financial reporting processes are generally tolerant of delay.

Availability and use of basic procedures and controls can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of financial reporting information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for financial reporting information is ***low***.

C.2.2.3 Budget and Finance Information Type

Budget and Finance includes the management of the Federal budget process including the development of plans and programs, budgets, and performance outputs and outcomes as well as financing Federal programs and operations through appropriation and apportionment of direct and reimbursable spending authority, fund transfers, investments and other financing mechanisms. Budget and financial management includes the establishment of a system for ensuring an organization does not obligate or disburse funds in excess of those appropriated or authorized. The recommended security categorization for the budget and finance information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)}

C.2.2.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of budget and finance information on the ability of responsible agencies to develop plans and programs, budgets, and performance outputs and outcomes; and to finance Federal programs and operations through appropriation and apportionment of direct and reimbursable spending authority, fund transfers, investments and other financing mechanisms.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of budget and finance information for programs that process classified or high-impact information can give adversaries damaging insights into details of agency plans, priorities, and operations. In relatively rare cases, actions taken based on unauthorized disclosure of funds management details can pose a threat to human life or a loss of major assets, so the confidentiality impact is ***high***. In general, unauthorized disclosure of budget and finance information, particularly of budget allocations for specific programs or program elements, can be seriously detrimental to government interests in procurement processes. In many instances, such unauthorized disclosure is prohibited by executive order or by law (e.g., *Federal Acquisition Regulations*). Premature release of draft budget and finance information can yield advantages to competing interests and seriously endanger agency operations – or even agency mission.

Recommended Confidentiality Impact Level: While, in many cases, unauthorized disclosure of funds management information will have only a limited adverse effect on agency operations, assets, or individuals, the potential for serious harm is such that the default confidentiality impact level recommended for budget and finance information is ***moderate***.

C.2.2.3.2 Integrity

Budget and finance activities are not generally time-critical. The consequences of unauthorized modification of budget and finance information can generally be overcome if mitigating procedures and controls are implemented. Although competent agency personnel should be able to recognize grossly anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives, an accumulation of small changes to data or deletion of small entries can result in budget shortfalls or cases of excessive obligations or disbursements that are not caught until after the fact audits.

Special Factors Affecting Integrity Impact Determination: While there is a potential for large-scale fraud, the checks and balances inherent in budget and finance processes significantly reduce the probability of successful fraudulent activities.

Recommended Integrity Impact Level: In most cases, the adverse effects of consequent negative publicity and institution of corrective action programs on mission functions, image or public confidence in the agency can be serious. Therefore, the default integrity impact recommended for budget and finance information is ***moderate***.

C.2.2.3.3 Availability

The effects of disruption of access to or use of budget and finance information can usually be repaired. The time frame required for repair is dependent on implementation and use of mitigating procedures and controls. Budget and finance processes are generally tolerant of delay. Availability and use of basic procedures and controls can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of budget and finance information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for budget and finance information is ***low***.

C.2.2.4 Accounting Information Type

Accounting entails accounting for assets, liabilities, fund balances, revenues and expenses associated with the maintenance of Federal funds and expenditure of Federal appropriations (Salaries and Expenses, Operation and Maintenance, Procurement, Working Capital, Trust Funds, etc.), in accordance with applicable Federal standards (FASAB, Treasury, OMB, GAO, etc.). The recommended security categorization for the accounting information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

C.2.2.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of accounting information on the abilities of government agencies to maintain Federal funds and expenditure of Federal appropriations in accordance with applicable Federal standards. Unauthorized disclosure of accounting information for programs that process classified or high-impact information can give adversaries damaging insights into details of agency plans, priorities, and operations.

Special Factors Affecting Confidentiality Impact Determination: In relatively rare cases, actions taken based on unauthorized disclosure of accounting details can pose a threat to human life or a loss of major assets, so the confidentiality impact is ***high***. In some cases, unauthorized disclosure of accounting information can violate proprietary information or other non-disclosure agreements. In such cases, the government may suffer, not only a loss of public confidence, but may become vulnerable to expensive and disruptive legal actions. Where sensitive or proprietary information is involved, the impact of unauthorized disclosure is likely to be ***moderate***. Where the accounting information is involved in an audit associated with suspected fraud or other criminal activities, the investigation may be imperiled. Here too, the impact of unauthorized disclosure is likely to be ***moderate***.

Recommended Confidentiality Impact Level: In most cases, unauthorized disclosure of accounting information will have only a limited adverse effect on agency operations, assets, or individuals. Therefore, the confidentiality impact level recommended for accounting information is ***low***.

C.2.2.4.2 Integrity

Accounting activities are not generally time-critical. The consequences of unauthorized modification of accounting information can generally be overcome if mitigating procedures and controls are implemented. Although competent agency personnel should be able to recognize grossly anomalous information and compare suspect information to that contained in source material, an accumulation of small changes to data or deletion of small entries can result in cost overruns and other cases of excessive obligations or disbursements that are not caught until after the fact audits.

Special Factors Affecting Integrity Impact Determination: In some cases, undetected integrity compromises can be extremely expensive to the government and its employees in terms of both monetary losses and loss of reputation. In most cases, the adverse effects of consequent negative publicity and institution of corrective action programs on mission functions and public confidence in the agency can be serious.

Recommended Integrity Impact Level: The default integrity impact recommended for accounting information is ***moderate***.

C.2.2.4.3 Availability

The effects of disruption of access to or use of accounting information can usually be repaired. The time frame required for repair is dependent on implementation and use of mitigating procedures and controls. Accounting processes are generally tolerant of delay. Availability and use of basic procedures and controls can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of accounting information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for accounting information is ***low***.

C.2.2.5 Payments Information Type

Payments include disbursements of Federal funds, via a variety of mechanisms, to Federal and private individuals, Federal agencies, state, local and international Governments, and the private sector, to effect payment for goods and services, or distribute entitlements, benefits, grants, subsidies, loans, or claims. Payment management provides appropriate control over all payments made by or on behalf of an organization, including but not limited to payments made to: vendors in accordance with contracts, purchase orders and other obligating documents; state governments under a variety of programs; employees for salaries and expense reimbursements; other Federal agencies for reimbursable work performed; individual citizens receiving Federal benefits; and recipients of Federal loans. The recommended security categorization for the payments information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

C.2.2.5.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of payments information on the ability of responsible agencies to provide appropriate control over all payments made by or on behalf of an organization. In most cases, unauthorized disclosure of payments information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for payments information is ***low***.

C.2.2.5.2 Integrity

Payments activities are not generally time-critical. The consequences of unauthorized modification of payments information can generally be overcome if mitigating procedures and controls are implemented. Although competent agency personnel should be able to recognize grossly anomalous information and compare suspect information to that contained in source material, an accumulation of small changes to data or deletion of small entries can result in cost overruns and other cases of excessive disbursements that are not caught until after the fact audits. In most cases, the adverse effects of consequent negative publicity and institution of corrective action programs on mission functions or public confidence in the agency can be serious.

Recommended Integrity Impact Level: The default integrity impact recommended for payments information is ***moderate***.

C.2.2.5.3 Availability

The effects of disruption of access to or use of payments information can usually be repaired. The time frame required for repair is dependent on implementation and use of mitigating procedures and controls. Payment processes are generally tolerant of delay. Availability and use of basic procedures and controls can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of payments information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for payments information is ***low***.

C.2.2.6 Collections and Receivables Information Type

Collections and Receivables include deposits, fund transfers, and receipts for sales or service. Receivable management supports activities associated with recognizing and recording debts due to the Government, performing follow-up actions to collect on these debts, and recording cash receipts. The recommended security categorization for the collections and receivables information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

C.2.2.6.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of collections and receivables information on the ability of responsible agencies to recognize and record debts due to the Government, perform follow-up actions to collect on these debts, and record cash receipts. In most cases, unauthorized disclosure of receivable management information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for collections and receivables information is ***low***.

C.2.2.6.2 Integrity

Collections and receivables activities are not generally time-critical. The consequences of unauthorized modification of collections and receivables information can generally be overcome if mitigating procedures and controls are implemented. Although competent agency personnel should be able to recognize grossly anomalous information and compare suspect information to that contained in source material, an accumulation of small changes to data or deletion of small entries can result in revenue shortfalls that are not caught until after the fact audits. In most cases, the adverse effects of consequent negative publicity and institution of corrective action programs on mission functions or public confidence in the agency can be serious.

Recommended Integrity Impact Level: The default integrity impact recommended for collections and receivables information is ***moderate***.

C.2.2.6.3 Availability

The effects of disruption of access to or use of collections and receivables information can usually be repaired. The time frame required for repair is dependent on implementation and use of adequate back up information, facilities and procedures. Collections and receivables processes are generally tolerant of delay. Availability and use of back-up files and alternate facilities can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of collections and receivables information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for collections and receivables information is ***low***.

C.2.3 Human Resources

Human resources activities involve all activities associated with the recruitment and management of personnel.

C.2.3.1 Benefits Management Information Type

Benefits management involves the administration of entitled benefits for federal personnel such as retirement, medical, disability, and insurance. The following security categorization is recommended for the benefits management information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.3.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of benefits management information on the abilities of responsible agencies to administer entitled benefits for federal personnel such as retirement, medical, disability, and insurance. The consequences of unauthorized disclosure of the vast majority of benefits management information will result in, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996, or information that is proprietary to a corporation or other organization (e.g., of insurers). In such cases, the consequences of unauthorized disclosure of benefits management information could be serious (particularly in cases of exposure of large data bases that might reveal private medical information or facilitate identity theft or other financial fraud). In such cases, the confidentiality impact level would be ***moderate***.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most benefits management information is ***low***.

C.2.3.2.2 Integrity

The consequences of unauthorized modification to or destruction of benefits management information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. Also, in the case of benefits management planning information, there is a high probability that an integrity compromise will be noticed before its consequences are felt. In any case, although there can be serious short-term effects for individuals, the effects of modifications to or deletion of this information are generally limited with respect to agency mission capabilities or assets. Any resulting damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for benefits management information is ***low***.

C.2.3.2.3 Availability

The effects of disruption of access to or use of benefits management information or information systems can usually be repaired within reasonable time and resource constraints. The time frame

required for repair is dependent implementation and use of mitigating procedures and controls. The nature of benefits management processes is tolerant of reasonable delays. In the case of benefits management records, the disruption of access to records can usually be overcome if back-up and archiving procedures are adequate and are implemented.

Recommended Availability Impact Level: The default availability impact level recommended for benefits management information is ***low***.

C.2.3.2 Personnel Management Information Type

Personnel Management involves the general management of the federal workforce, including but not limited to functions such as personnel action processing, employee tracking, position classification and management, discipline/grievance, advancement and awards, labor relations, etc. The following security categorization is recommended for the personnel management information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.3.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of personnel management information on the abilities of responsible agencies to manage the federal workforce. The consequences of unauthorized disclosure of the vast majority of personnel management information will result in, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996, or other laws and executive orders affecting the dissemination of information regarding individuals. In such cases, the consequences of unauthorized disclosure of personnel management information could be serious, particularly in cases of exposure of data that might facilitate identity theft or support extortion (e.g., unauthorized disclosure of legal, financial, or moral misbehavior by Federal employees). In such cases, the confidentiality impact level might be ***moderate***.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most personnel management information is ***low***.

C.2.3.2.2 Integrity

The consequences of unauthorized modification to or destruction of personnel management information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. Also, in the case of personnel management planning information, there is a high probability that an integrity compromise will be noticed before its consequences are felt. In any case, although there can be serious short-term effects for individuals, the effects of modifications to or deletion of this information are generally limited with respect to agency mission capabilities or assets. Any resulting damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for personnel management information is ***low***.

C.2.3.2.3 Availability

The effects of disruption of access to or use of personnel management information or information systems can usually be repaired within reasonable time and resource constraints. The time frame required for repair is dependent implementation and use of mitigating procedures and controls. The nature of personnel management processes is tolerant of reasonable delays. In the case of personnel management records, the disruption of access to records can usually be overcome if basic procedures and controls are implemented.

Recommended Availability Impact Level: The default availability impact level recommended for personnel management information is ***low***.

C.2.3.3 Payroll Management and Expense Reimbursement Information Type

Payroll management and expense reimbursement involves the administration and determination of federal employee compensation. Note: See *payments* information type for the actual payment of salary and expenses. The recommended security categorization for the payroll management and expense reimbursement information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.3.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of payroll management and expense reimbursement information on the ability of responsible agencies to administer and determine Federal employee compensation. In most cases, unauthorized disclosure of payroll management and expense reimbursement information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for payroll management and expense reimbursement information is ***low***.

C.2.3.3.2 Integrity

Payroll management and expense reimbursement activities are not generally time-critical. The consequences of unauthorized modification of payroll management and expense reimbursement information can generally be overcome if mitigating procedures and controls are implemented.

Special Factors Affecting Integrity Impact Determination: Although competent agency personnel should be able to recognize grossly anomalous information and compare suspect information to that contained in source materials, an accumulation of small changes to data or deletion of small entries can result in excessive disbursements that are not caught until after the fact audits. In many cases, the adverse effects of consequent negative publicity and institution of

corrective action programs on mission functions or public confidence in the agency can be serious.

Recommended Integrity Impact Level: In most cases, the default integrity impact recommended for payroll management and expense reimbursement information is ***low***.

C.2.3.3.3 Availability

The effects of disruption of access to or use of payroll management and expense reimbursement information can usually be repaired. The time frame required for repair is dependent on implementation and use of mitigating procedures and controls. Payment processes are generally tolerant of delay. Availability and use of basic procedures and controls can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of payroll management and expense reimbursement information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for payroll management and expense reimbursement information is ***low***.

C.2.3.4 Resource Training and Development Information Type

Resource training and development refers to the active building of capacities in staff members through formal, technical, or other means of education. The recommended security categorization for the resource training and development information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.3.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of resource training and development information on the ability of responsible agencies to build capacities in staff members through formal, technical, or other means of education. In most cases, unauthorized disclosure of resource training and development information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for resource training and development information is ***low***.

C.2.3.4.2 Integrity

The consequences of unauthorized modification to or destruction of resource training and development information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. Also, in the case of resource training and development planning information, there is a high probability that an integrity compromise will be noticed before its consequences are felt. In any case, although there can be serious short-term effects for individuals, the effects of modifications to or deletion

of this information are generally limited with respect to agency mission capabilities or assets. Any resulting damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for resource training and development information is ***low***.

C.2.3.4.3 Availability

The effects of disruption of access to or use of resource training and development information or information systems can usually be repaired within reasonable time and resource constraints. The time frame required for repair is dependent implementation and use of mitigating procedures and controls. The nature of resource training and development processes is tolerant of reasonable delays. In the case of resource training and development records, the disruption of access to records can usually be overcome if basic procedures and controls are implemented.

Recommended Availability Impact Level: The default availability impact level recommended for resource training and development information is ***low***.

C.2.3.5 Security Clearance Management Information Type

Security clearance management refers to the processes associated with ensuring employees, contractors, and others have been approved to enter Federal buildings, utilize Federal services, and access sensitive information. This includes eligibility determination, badge issuance, clearance tracking, and security verification services. Note that impacts to some information and information systems associated with security clearance management may inherently affect the security of critical infrastructures and key national assets. Note also that, although much information associated with security clearance management is national security related (hence outside the scope of this guideline), security clearance as used in this guideline is not restricted to national security applications. The following security categorization is recommended for the security clearance information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.3.5.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of security clearance information on the abilities of responsible agencies to manage access eligibility determination, badge issuance, clearance tracking, and security verification services for Federal information and facilities. The consequences of unauthorized disclosure of the vast majority of security clearance information can facilitate attempts by terrorists, other criminals, and other unauthorized individuals to enter Federal buildings, utilize Federal services, and access sensitive information. The consequences can range from limited loss of public confidence in an agency to serious or catastrophic adverse effects on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where terrorist acts are enabled, the confidentiality impact must be assumed to be ***high***. In cases of critical infrastructure facilities, key national assets, law enforcement facilities, and homeland security facilities, the confidentiality impact must generally be assumed to be ***high***. Unauthorized disclosure of

personal information subject to the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996, or other laws and executive orders affecting the dissemination of information regarding individuals can facilitate identity theft or support extortion (e.g., unauthorized disclosure of legal, financial, or moral misbehavior by Federal employees). In such cases, the confidentiality impact level might be ***moderate***.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most security clearance information that does not permit access to national security facilities or information is ***moderate***.

C.2.3.5.2 Integrity

The consequences of unauthorized modification to or destruction of security clearance information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. Modified security clearance information can be used to facilitate attempts by terrorists, other criminals, and other unauthorized individuals to enter Federal buildings, utilize Federal services, and access sensitive information. The consequences can range from limited loss of public confidence in an agency to serious or catastrophic adverse effects on agency operations, agency assets, or individuals.

Special Factors Affecting Integrity Impact Determination: Where terrorist acts are enabled, the integrity impact must be assumed to be ***high***. In cases of critical infrastructure facilities, key national assets, law enforcement facilities, and homeland security facilities, the integrity impact must generally be assumed to be ***high***. In the case of security clearance information, there is not a sufficiently high probability that an integrity compromise will be noticed before its consequences are felt. It cannot be assumed that the effects of modifications to or deletion of security clearance information will be generally limited with respect to agency mission capabilities or assets.

Recommended Integrity Impact Level: The default integrity impact level recommended for most security clearance information is ***moderate***.

C.2.3.5.3 Availability

The time frame required for repair effects of disruption of access to or use of security clearance information or information systems is dependent implementation and use of mitigating procedures and controls. Loss of availability of security clearance information may result in general denial of access to Federal government facilities and information for which clearance is required until access to verifiably correct clearance information is restored. While the nature of security clearance processes is tolerant of reasonable delays, the processes that use the clearance information to grant or deny access are often not so tolerant of disruption.

Recommended Availability Impact Level: The default availability impact level recommended for security clearance information is ***moderate***.

C.2.3.6 Staff Recruitment and Employment Information Type

Staff recruitment and employment refers to the active marketing and hiring of personnel to fill opportunities and vacancies within an organization. The recommended security categorization for the staff recruitment and employment information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.3.6.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of staff recruitment and employment information on the ability of responsible agencies to market and hire personnel to fill opportunities and vacancies within an organization. In most cases, unauthorized disclosure of staff recruitment and employment information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for staff recruitment and employment information is ***low***.

C.2.3.6.2 Integrity

The consequences of unauthorized modification to or destruction of staff recruitment and employment information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. Also, in the case of staff recruitment and employment planning information, there is a high probability that an integrity compromise will be noticed before its consequences are felt. In any case, although there can be serious short-term effects for individuals, the effects of modifications to or deletion of this information are generally limited with respect to agency mission capabilities or assets. Any resulting damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for staff recruitment and employment information is ***low***.

C.2.3.6.3 Availability

The effects of disruption of access to or use of staff recruitment and employment information or information systems can usually be repaired within reasonable time and resource constraints. The time frame required for repair is dependent implementation and use of mitigating procedures and controls. The nature of staff recruitment and employment processes is tolerant of reasonable delays. In the case of staff recruitment and employment records, the disruption of access to records can usually be overcome if basic procedures and controls are implemented.

Recommended Availability Impact Level: The default availability impact level recommended for staff recruitment and employment information is ***low***.

C.2.4 Supply Chain Management

Supply chain management involves the purchasing, tracking, and overall management of goods and services.

C.2.4.1 Goods Acquisition Information Type

Goods acquisition involves the procurement of physical goods, products, and capital assets to be used by the Federal government. The recommended security categorization for the goods acquisition information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.4.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of goods acquisition information on the ability of agencies to procure physical goods, products, and capital assets to be used by the Federal government. The consequences of unauthorized disclosure of most goods acquisition information are likely to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of information associated with very large procurements can result in fraud, waste, abuse, and/or legal proceedings that can have a serious to severe effect on Federal government assets and operations. Also, information associated with acquisition of many Federal government facilities can be of material use to criminals seeking to gain access to those facilities in order to facilitate or perpetrate fraud, theft, or some other criminal enterprise. In this case, unauthorized disclosure of information can have a serious adverse effect on agency operations, agency assets, or individuals. The consequent confidentiality impact would range from ***moderate*** to ***high***. Note that some procurement information is classified. The classified information is *national security related* and is outside the scope of this guideline. Also, either anticipated or realized unauthorized disclosure of one agency's goods acquisition information by another agency could result in negative impacts on cross-jurisdictional coordination within the goods acquisition infrastructure and the general effectiveness of organizations tasked with acquisition of government facilities and supplies.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most goods acquisition information is ***low***.

C.2.4.1.2 Integrity

The consequences of unauthorized modification to or destruction of goods acquisition information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately. The consequences of unauthorized modification to or destruction of goods acquisition information can generally be overcome if basic procedures and controls implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external publication of goods acquisition information (e.g., web pages, electronic mail) may adversely affect public confidence in the agency. However, damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most goods acquisition information is ***low***.

C.2.4.1.3 Availability

The effects of disruption of access to or use of goods acquisition information or information systems can usually be expected to be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of functions supported by most goods acquisition information is tolerant of delays.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency procurements necessary to support response aspects of disaster management. In such cases, delays measured in hours can cost lives and major property damage. Consequently, the availability impact level associated with unauthorized modification or destruction of goods acquisition information needed to respond to emergencies can be ***high***. The more common case is likely to be that disruption of access has a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: In general, given implementation and use of basic procedures and controls, and where processes to which the information is essential are either not time-critical or not likely to have serious or severe consequences, the default availability impact level recommended for goods acquisition information is ***low***.

C.2.4.2 Inventory Control Information Type

Inventory control refers to the tracking of information related to procured assets and resources with regards to quantity, quality, and location. The recommended security categorization for the inventory control information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.4.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of inventory control information on the ability of agencies to track information related to procured assets and resources with regards to quantity, quality, and location. The consequences of unauthorized disclosure of most inventory control information are likely to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of information associated with inventories of hazardous materials (e.g., radioactive materials, toxins, bio-hazardous items, explosives) can facilitate terrorist or other criminal activities that

can result in serious to severe effects on Federal government assets and operations and on the general public. Inventory control information in general can be of material use to criminals seeking to perpetrate fraud, theft, or some other criminal enterprise. In these cases too, unauthorized disclosure of information can have a serious adverse effect on agency operations, agency assets, or individuals. The consequent confidentiality impact of these types of criminal exploitation of unauthorized disclosure of inventory control information would range from ***moderate*** to ***high***. Note that some inventory control information is classified. The classified information is *national security related* and is outside the scope of this guideline. Also, either anticipated or realized unauthorized disclosure of one agency's inventory control information by another agency could result in negative impacts on cross-jurisdictional coordination within the inventory control infrastructure and the general effectiveness of organizations tasked with distribution and accounting of government facilities and supplies.

Recommended Confidentiality Impact Level: In spite of the aforementioned cases where there is ***moderate*** or ***high*** impact associated with unauthorized disclosure of inventory control information, the default confidentiality impact level recommended for most inventory control information is ***low***.

C.2.4.2.2 Integrity

The consequences of unauthorized modification to or destruction of inventory control information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately. The consequences of unauthorized modification to or destruction of inventory control information can generally be overcome if mitigating procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external publication of inventory control information (e.g., web pages, electronic mail) may adversely affect public confidence in the agency. However, damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most inventory control information is ***low***.

C.2.4.2.3 Availability

The effects of disruption of access to or use of inventory control information or information systems can usually be expected to be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of functions supported by most inventory control information is tolerant of delays.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency requirements to access and distribute materials necessary to support response aspects of disaster management. In such cases, delays measured in hours can cost lives and

major property damage. Consequently, the availability impact level associated with non-availability of inventory control information needed to respond to emergencies can be ***high***. The more common case is likely to be that disruption of access has a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: In general, given implementation and use of basic procedures and controls, and where processes to which the information is essential are either not time-critical or not likely to have serious or severe consequences, the default availability impact level recommended for inventory control information is ***low***.

C.2.4.3 Logistics Management Information Type

Logistics management involves the planning and tracking of personnel and their resources in relation to their availability and location. The recommended security categorization for the logistics management information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.4.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of logistics management information on the ability of agencies to plan and track personnel and their resources in relation to their availability and location. The consequences of unauthorized disclosure of most logistics management information in most agencies are likely to have only limited adverse effects on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of logistics information associated with homeland security, law enforcement and some transportation activities (e.g., air transport) can facilitate terrorist or other criminal activities that can result in serious to severe effects on Federal government assets and operations and on the general public. Logistics management information associated with a broad range of mission areas can be of material use to criminals seeking to perpetrate fraud, theft, or some other criminal enterprise. It is a key intelligence target for those seeking information of defense or law enforcement capabilities, dispositions and intent. In these cases too, unauthorized disclosure of logistics management information can result in serious adverse effects on agency operations, agency assets, and individuals. The consequent confidentiality impact of these types of criminal exploitation of unauthorized disclosure of logistics management information would range from ***moderate*** to ***high***. Note that some logistics management information is classified (e.g., some military logistics information). The classified information is *national security related* and is outside the scope of this guideline.

Recommended Confidentiality Impact Level: In spite of the aforementioned cases where there is ***moderate*** or ***high*** impact associated with unauthorized disclosure of logistics management information, the default confidentiality impact level recommended for most logistics management information is ***low***.

C.2.4.3.2 Integrity

The consequences of unauthorized modification to or destruction of logistics management information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately. The consequences of unauthorized modification to or destruction of logistics management information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external publication of logistics management information (e.g., web pages, electronic mail) may adversely affect public confidence in the agency. However, damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most logistics management information is ***low***.

C.2.4.3.3 Availability

The effects of disruption of access to or use of logistics management information or information systems can usually be expected to be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of functions supported by most logistics management information is tolerant of delays.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency requirements to deploy personnel and their resources to support response aspects of disaster management. In such cases, delays measured in hours can cost lives and major property damage. Consequently, the availability impact level associated with non-availability of logistics management information needed to respond to emergencies can be ***high***. The more common case is likely to be that disruption of access to logistics management information has only a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: In general, given implementation and use of basic procedures and controls, and where processes to which the information is essential are either not time-critical or not likely to have serious or severe consequences, the availability impact level recommended for logistics management information is ***low***.

C.2.4.4 Services Acquisition Information Type

Services acquisition involves the oversight and/or management of contractors and service providers from the private sector. The recommended security categorization for the services acquisition information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.4.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of services acquisition information on the ability of agencies to oversee and/or manage contractors and service providers from the private sector. The consequences of unauthorized disclosure of most services acquisition information are likely to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of information associated with very large procurements can result in fraud, waste, abuse, and/or legal proceedings that can have a serious to severe effect on Federal government assets and operations. Also, information associated with acquisition of some services (e.g., security or protection services) can be of material use to criminals seeking to gain access to Federal facilities or information in order to facilitate or perpetrate sabotage, murder, fraud, theft, or some other criminal enterprise. In this case, unauthorized disclosure of information can have a serious to severe adverse effect on agency operations, agency assets, and/or individuals. The consequent confidentiality impact would range from ***moderate*** to ***high***. Note that some services procurement information is classified. The classified information is *national security related* and is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most services acquisition information is ***low***.

C.2.4.4.2 Integrity

The consequences of unauthorized modification to or destruction of services acquisition information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately. The consequences of unauthorized modification to or destruction of services acquisition information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external publication of services acquisition information (e.g., web pages, electronic mail) may adversely affect public confidence in the agency. However, damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most services acquisition information is ***low***.

C.2.4.1.3 Availability

The effects of disruption of access to or use of services acquisition information or information systems can usually be expected to be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of functions supported by most services acquisition information is tolerant of

delays. In most cases, disruption of access to services procurement information can be expected to have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: In general, given implementation and use of basic procedures and controls, the default availability impact level recommended for services acquisition information is ***low***.

C.2.5 Information and Technology Management

IT management involves the coordination of information technology resources and systems required to support or enable a citizen service. Impacts to information associated with the operation of IT systems generally need to be considered even when all mission-related information processed by the system is intended to be available to the general public. The relevant issues may be different for integrity and availability than for confidentiality. Information that has been made public, by definition, requires no confidentiality protection. Integrity protection cannot necessarily be maintained for copies (or instantiations) of information that have been distributed to the public (have been distributed beyond the control of the originating/controlling organization's systems). Availability protection cannot necessarily be maintained for those copies/instantiations for the same reasons. It may be that only by maintaining copies of information in organization-controlled or operated information systems can integrity and availability assurance be established and/or maintained.

C.2.5.1 System Development Information Type

System Development supports all activities associated with the in-house design and development of software applications. The recommended security categorization for the system development information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

C.2.5.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of system development information on the ability of responsible agencies to design and design and develop software applications in-house. It is in the system development phase that a systems security configuration baseline is established. In most cases, the system development information is not particularly sensitive. It is distributed to the users. In general, unless the computer software itself is sensitive (e.g., classified algorithms associated with some software used in national security applications), disclosure of the system development information is likely to result in only limited adverse effects on the confidentiality and integrity of system information and processes.

Recommended Confidentiality Impact Level: The recommended impact level for system development information is ***low***.

C.2.5.1.2 Integrity

The consequences of unauthorized modification to or destruction of system development information can be particularly serious because modifications are very difficult to detect. The

consequences of undetected and unauthorized modification to or destruction of system development information depend on the maximum aggregate sensitivity and criticality of the end information and processes associated with the use of the end system. The recommended integrity impact level can range from ***low*** to ***high*** to *national security information* (outside the scope of this guideline).

Recommended Integrity Impact Level: Subject to the caveats above, the default integrity impact level associated with modification or destruction of system development information is ***moderate***.

C.2.5.1.3 Availability

The consequences of unauthorized modification or destruction of system development information can generally be overcome if basic mitigating procedures and controls are implemented. Temporary disruption of access to system development information can usually be expected to have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Permanent disruption of access would mean loss of the configuration baseline, the basis for security configuration management.

Recommended Availability Impact Level: In general, where processes to which the system development information is essential are either not time-critical or not likely to have serious or severe consequences, the default availability impact level recommended for system development information is ***low***.

C.2.5.2 Lifecycle/Change Management Information Type

Lifecycle/Change Management involves the processes that facilitate a smooth evolution, composition, and workforce transition of the design and implementation of changes to agency resources such as assets, methodologies, systems, or procedures. The recommended security categorization for the lifecycle/change management information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

C.2.5.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of lifecycle/change management information on the ability of responsible agencies to execute processes that facilitate a smooth evolution, composition, and workforce transition of the design and implementation of changes to agency resources such as assets, methodologies, systems, or procedures. It is in the lifecycle/change management phase that a systems security configuration management occurs.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some lifecycle/change management information can equip adversaries with intelligence information that may be useful to efforts to compromise the confidentiality and/or integrity of the system. This is because during lifecycle/change management malicious or unintended

vulnerabilities can result from configuration changes and lifecycle/change management procedures and mechanisms (e.g., version control, back-up, access control, and configuration audit procedures) are employed to detect flaws and malicious code.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for lifecycle/change management information is ***low***.

C.2.5.2.2 Integrity

The consequences of unauthorized modification to or destruction of lifecycle/change management information can be particularly serious because modifications are very difficult to detect. The consequences of undetected and unauthorized modification to or destruction of lifecycle/change management information depends on the maximum aggregate sensitivity and criticality of the end information and processes associated with the use of the end system. The recommended integrity impact level can range from ***low*** to ***high*** to *national security information* (outside the scope of this guideline).

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of lifecycle/change management information is ***moderate.***

C.2.5.2.3 Availability

The consequences of unauthorized modification or destruction of lifecycle/change management information can generally be overcome if basic mitigating procedures and controls are implemented. Temporary disruption of access to lifecycle/change management information can usually be expected to have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Permanent disruption of access would mean failure of configuration management.

Recommended Availability Impact Level: In general, where processes to which lifecycle/change management information is essential are either not time-critical or not likely to have serious or severe consequences, the default availability impact level recommended for lifecycle/change management information is ***low***.

C.2.5.3 System Maintenance Information Type

System Maintenance supports all activities associated with the maintenance of in-house designed software applications. The recommended security categorization for the system maintenance information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

C.2.5.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of system maintenance information on the ability of responsible agencies to maintain in-house designed software applications. In the system maintenance phase, that changes requiring configuration

management processes are made. In most cases, the system maintenance information is not particularly sensitive. It is distributed to the users. In general, unless the computer software itself is sensitive (e.g., classified algorithms associated with some software used in national security applications), disclosure of the system maintenance information is likely to result in only limited adverse effects on the confidentiality and integrity of system information and processes.

Recommended Confidentiality Impact Level: The recommended impact level for system maintenance information is ***low***.

C.2.5.3.2 Integrity

The consequences of unauthorized modification to or destruction of system maintenance information can be particularly serious because modifications to system changes can be subtle and very difficult to detect. The consequences of undetected and unauthorized modification to or destruction of system maintenance information may depend on the maximum aggregate sensitivity and criticality of the end information and processes associated with the use of the end system. The recommended integrity impact level can range from ***low*** to ***high*** to *national security information* (outside the scope of this guideline).

Recommended Integrity Impact Level: Subject to the caveats above, the default integrity impact level recommended for modification or destruction of system maintenance information is ***moderate***.

C.2.5.3.3 Availability

The consequences of unauthorized modification or destruction of system maintenance information can generally be overcome if basic mitigating procedures and controls are implemented. Disruption of access to system maintenance information can usually be expected to have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: In general, where processes to which system maintenance information is essential are either not time-critical or not likely to have serious or severe consequences, the default availability impact level recommended for system maintenance information is ***low***.

C.2.5.4 IT Infrastructure Management Information Type

IT infrastructure maintenance involves the planning, design, implementation, and maintenance of an IT Infrastructure to effectively support automated needs (i.e. operating systems, applications software, platforms, networks, servers, printers, etc.). IT infrastructure maintenance also includes information systems configuration and security policy enforcement information. This information includes password files, file access tables, network access rules and implementing files and/or switch setting, and other hardware and software configuration settings and documentation that may affect access to the information system's data, programs, and/or processes. The impact levels associated with IT infrastructure maintenance information are primarily a function of the information processed in and through that infrastructure. Where the confidentiality, integrity, and availability impact levels associated with the information processed

by an IT infrastructure are all ***low***, the recommended security categorization for the IT infrastructure maintenance information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.5.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of IT infrastructure maintenance information on the ability of responsible agencies to plan, design, implement, and maintain an IT Infrastructure to effectively support automated needs (i.e. operating systems, applications software, platforms, networks, servers, printers, etc.). [See also Appendices C.2.5.5, IT Security Information and C.2.5.7, Information Management Information.] IT infrastructure maintenance also includes information systems configuration and security policy enforcement information. Unauthorized disclosure of some IT infrastructure maintenance information can lead to confidentiality and/or integrity compromise of any or all information processed by the system (e.g., password files, file access tables, cryptographic keying information, network access rules and implementing files and/or switch setting, and other hardware and software configuration settings and documentation that may affect access to the information system's data, programs, and/or processes). As a result, the confidentiality impact associated with this information is that of the highest impact information processed by the system. Note also that a higher confidentiality impact may be associated with information in aggregate than is associated with any single element of information.

Recommended Confidentiality Impact Level: Only if the confidentiality levels associated with all the information processed by an IT infrastructure (individuality and in aggregate) are ***low***, the recommended default impact level recommended for IT infrastructure maintenance information is ***low***.

C.2.5.4.2 Integrity

The consequences of unauthorized modification to or destruction of IT infrastructure maintenance information usually depends on the urgency with which the information processed in and through the IT infrastructure is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately. In relatively few cases would the consequences of unauthorized modification of IT infrastructure maintenance information that is acted upon immediately result in more than limited damage to agency operations or assets.

Special Factors Affecting Integrity Impact Determination: Exceptions may include bogus information necessary to operation of communications processors, data base systems, or other systems necessary to emergency response aspects of disaster management, criminal apprehension, air traffic control or other time-critical missions. In such cases, a ***moderate*** or ***high*** integrity impact level might be considered for unauthorized modification or destruction of IT infrastructure maintenance information. The consequences of unauthorized modification to or destruction of IT infrastructure maintenance information also depend on mitigating procedures and controls. The consequences of unauthorized modification or destruction of much IT infrastructure maintenance information can generally be overcome if basic procedures and controls are adequate and are implemented.

Recommended Integrity Impact Level: Subject to the caveats above, the default integrity impact level recommended for modification or destruction of IT infrastructure maintenance information is ***low***.

C.2.5.4.3 Availability

The effects of disruption of access to or use of IT infrastructure maintenance information or information systems can usually be expected to deny mission-critical IT resources to all affected agencies. However, the consequences of unauthorized modification or destruction of much IT infrastructure maintenance information can generally be overcome if basic mitigating procedures and controls are implemented. In most such cases, infrastructure functionality can be restored in time to prevent catastrophic loss.

Special Factors Affecting Availability Impact Determination: Exceptions may include emergency response aspects of disaster management or other high load and time critical functions (e.g., some systems that support air traffic control functions). The availability impact level associated with unauthorized modification or destruction of IT infrastructure maintenance information needed to respond to emergencies or critical to public safety can be ***high***. The far more common case is likely to be that disruption of access has a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: In general, where processes to which the information is essential are either not time-critical or not likely to have serious or severe consequences, the default availability impact level recommended for IT infrastructure maintenance information is ***low***.

C.2.5.5 IT Security Information Type

IT Security involves all functions pertaining to the securing of Federal data and systems through the creation and definition of security policies, procedures and controls covering such services as identification, authentication, and non-repudiation. The general recommended security categorization for the IT security information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

C.2.5.5.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of IT security information on the ability of responsible agencies to secure Federal data and systems through the creation and definition of security policies, procedures and controls covering such services as identification, authentication, and non-repudiation. It is in the IT security phase that a systems security policy is established and the implementation of the policy is defined. In most cases, the security policy, procedures, and available controls are not particularly sensitive. It is the variable security information used in initializing and implementing the controls (e.g., passwords, cryptographic keys) that need to be protected. In general, disclosure of the security policies, procedures, and controls can result in only limited adverse effects on the confidentiality and integrity of system information and processes.

Recommended Confidentiality Impact Level: The recommended default impact level for IT security information is ***low***.

C.2.5.5.2 Integrity

The consequences of unauthorized modification or destruction of IT security information depends, in large part, on mitigating procedures and controls. The consequences of unauthorized modification or destruction of IT security information can usually be overcome if basic procedures and controls are implemented. In many cases, competent agency personnel should be able to recognize anomalous information (e.g., by comparing suspect information to that contained in source material, back-up files, and/or archives). Damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for IT security information is ***low***.

C.2.5.5.3 Availability

The consequences of unauthorized modification or destruction of IT security information can generally be overcome if basic mitigating procedures and controls are implemented. Temporary disruption of access to IT security information can usually be expected to have a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: Permanent disruption of access would mean loss of the configuration baseline, the basis for security configuration management.

Recommended Availability Impact Level: In general, where processes to which the IT security information is essential are either not time-critical or not likely to have serious or severe consequences, the availability impact level recommended for IT security information is ***low***.

C.2.5.6 Record Retention Information Type

Records Retention involves the operations surrounding the management of the official documents and records for an agency. Subject to exception conditions described below, the recommended security categorization for the record retention information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

C.2.5.6.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of record retention information on the ability of responsible organizations to store, track, account for, maintain, retrieve, and disseminate official documents and records. Note that *national security information* and *national security systems* are outside the scope of this guideline. Otherwise, where the data being retained belongs to one of the information types described in this guideline, the confidentiality impact assigned the data and system is at least that of the highest impact information type collected. In some cases, it is necessary for impact assessment to consider the

possibility that the aggregate of information retained will have a higher confidentiality impact than any individual information element or type. Note that unauthorized disclosure of security policies and practices can provide some assistance to an adversary attempting to gain access to agency information. Unauthorized disclosure of access control information (e.g., configuration settings, passwords, authorization codes, cryptographic keys) can assist or even enable an attack. It is anticipated that unauthorized disclosure of most business management information retained will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974 or information that is proprietary to a corporation or other organization. Such information will often be assigned a ***moderate*** confidentiality impact level. Where any of the information to be collected can reasonably be expected to have a ***high*** confidentiality impact level, then the record retention system must be assigned a ***high*** confidentiality impact level.

Recommended Confidentiality Impact Level: In general, the default confidentiality impact level recommended for record retention information is ***low***.

C.2.5.6.2 Integrity

The consequences of unauthorized modification or destruction of record retention information depends, in large part, on mitigating procedures and controls. The consequences of unauthorized modification or destruction of record retention information can usually be overcome if basic procedures and controls are implemented. In many cases, competent agency personnel should be able to recognize anomalous information (e.g., by comparing suspect information to that contained in source material, back-up files, and/or archives).

Special Factors Affecting Integrity Impact Determination: In the absence of adequate back-up procedures, loss of integrity for some access control information (e.g., encryption keys) can be catastrophic for agency operations. Where the consequences involve erroneous or fraudulent business management information, eventual successful corrective action can be anticipated. Where the results take the form of delays in or denial of service, there can be more serious consequences for public confidence in the agency. Damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: In general, the integrity impact level recommended for record retention information is ***low***.

C.2.5.6.3 Availability

The effects of disruption of access to or use of record retention information can usually be repaired. The time frame required for repair is dependent on implementation and use of mitigating procedures and controls. Record retention processes are generally tolerant of reasonable delays. Availability and use of basic procedures and controls can be relied upon to prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of record retention information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: In the absence of basic procedures and controls (e.g., back-up), loss of availability for some access control information (e.g., encryption keys) can be catastrophic for agency operations. Not many business management systems perform functions for which temporary loss of availability can cause significant degradation in or loss of mission capability, place the agency at a significant disadvantage, result in major damage to or loss of major assets, or pose a threat to human life.

Recommended Availability Impact Level: The default availability impact recommended for record retention information is ***low***.

C.2.5.7 Information Management Information Type

Information Management involves the coordination of information collection, storage, and dissemination, and destruction as well as managing the policies, guidelines, and standards regarding information management. Subject to exception conditions described below, the general recommended security categorization for the information management information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW[9]), (**integrity**, MODERATE), (**availability**, LOW)}

C.2.5.7.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of information management information on the ability of responsible agencies to perform the day-to-day processes of information collection, storage, and dissemination, and destruction as well as managing the policies, guidelines, and standards regarding information management. The consequences of unauthorized disclosure depend largely on the content and use of the information being managed. Note that national *security information* and *national security systems* are outside the scope of this guideline. Otherwise, where the data being managed belongs to one of the information types described in this guideline, the confidentiality impact assigned the data and system is that of the highest impact information type processed by the system. Depending on the agency and the mission being supported, the sensitivity of the information can range from none (public information) to ***high***.

Special Factors Affecting Confidentiality Impact Determination: Information collection and storage involve the day-to-day processes of gathering and storing data from agency programs, partners, and stakeholders. It is anticipated that unauthorized disclosure of information management information that governs the processing of most information managed by the government will have only a limited adverse effect on agency operations, assets, or individuals. Where more sensitive information is being managed, it will most commonly be personal information subject to the Privacy Act of 1974 or information that is proprietary to a corporation or other organization. Such information will often be assigned a ***moderate*** confidentiality impact level. Information dissemination involves managing the permissions and connections required to share data both inside and outside of an agency. The level of confidentiality impact associated

[9] Confidentiality impact for access control information is that of the highest confidentiality, integrity, or availability impact level assigned to any information that may be processed by the system.

with information sharing information is generally associated with its effect on the ability of responsible agencies to manage the permissions and connections required to share (and/or destroy) data both inside and outside of an agency. This information includes processor and network configuration settings, passwords, authorization codes, and cryptographic keys. Where there is a reasonable probability of serious adverse effects on agency operations or individuals due to consequences of exposure of this information, related information management information will often be assigned a ***moderate*** confidentiality impact level. Where any of the information to be managed can reasonably be expected to have a ***high*** confidentiality, integrity, or availability impact level, then the information sharing information must be assigned a ***high*** confidentiality impact level.

Recommended Confidentiality Impact Level: In the absence of a specific basis for assigning a ***moderate*** or ***high*** sensitivity level to information being managed by a system, the default confidentiality impact level recommended for information sharing information in most systems is ***low***.

C.2.5.7.2 Integrity

The consequences of unauthorized modification or destruction of information management information (e.g., configuration settings, passwords, authorization codes, cryptographic keying material) can compromise the effectiveness of the host system and impair agency operations. The level of impact depends on the criticality of system functionality to the agency mission and on mitigating procedures and controls. [Note that most back-up and archiving procedures are designed to work with copies of data as collected and introduced into the system.] The consequences of unauthorized modification or destruction of information management information can usually be overcome within reasonable time and resource constraints if basic procedures and controls are implemented. However, in most cases, agency personnel cannot be expected to recognize anomalous management information and compare suspect information to that contained in original sources.

Special Factors Affecting Integrity Impact Determination: The consequences can be particularly serious if the destruction or modification of information renders confidentiality mechanisms that protect high-impact information ineffective. In the absence of basic procedures and controls, loss of integrity for some information sharing information (e.g., encryption keys) can be catastrophic for agency operations. A resulting requirement to rebuild an agency database can create long-term delays in or effective denial of service. This can be expected to have serious or severe consequences for agency operations or public confidence in the agency. Damage can generally be corrected in time, but the resource requirements can be prohibitive. The relationship between integrity impact level and basic integrity control mechanisms is particularly strong in the case of information management information. The sensitivity and criticality of the data processed in the system employing the information management information will be a primary factor in determining selection of integrity controls. The integrity impact level recommended for information management information associated with highly critical information is ***high***.

Recommended Integrity Impact Level: Although, the integrity impact resulting from unauthorized modification or deletion of management information or processes depends on the

sensitivity and criticality of the information and processes being supported, potentially serious adverse effects can be expected in most government organizations. Therefore, at least a ***moderate*** default integrity impact level is recommended for management information.

C. 2.5.7.3 Availability

The effects of disruption of access to or use of information management information (e.g., configuration settings, passwords, authorization codes, cryptographic keys) can at least temporarily destroy the effectiveness of the host system and impair agency operations. The level of impact depends on the sensitivity of the information being managed, the criticality of system functionality to the agency mission, and the mitigating procedures and controls. Except for possible cases of information needed by real-time processes (e.g., information that feeds real-time monitoring or audit functions), information management processes are generally tolerant of reasonable delays. Availability and use of basic procedures and controls (e.g., alternate communications and input media) can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of collection information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals. Not many business management systems perform functions for which loss of availability can cause significant degradation in or loss of mission capability, place the agency at a significant disadvantage, result in major damage to or loss of major assets, or pose a threat to human life.

Special Factors Affecting Availability Impact Determination: Particularly in the cases of monitoring and audit functions, loss of availability can result in permanent loss of some information on which system operation is dependent. In most systems and systems applications, the consequences of disruption of access to or use of information management information can usually be overcome if basic procedures and controls are implemented. In the absence of basic procedures and controls, loss of availability for some information sharing information (e.g., encryption keys) can be catastrophic for agency operations. A resulting requirement to rebuild an agency database can create long-term delays in or effective denial of service. This can be expected to have serious or severe consequences for agency operations or public confidence in the agency. In most cases, damage can eventually be corrected, but the resource required can be prohibitive.

Recommended Availability Impact Level: In the case of most Federal government information systems, given implementation and use of basic procedures and controls (e.g., well-defined and rigorously implemented back-up procedures), the default integrity impact level recommended for information sharing information is ***low***.

APPENDIX D: EXAMPLES OF IMPACT DETERMINATION FOR AGENCY-SPECIFIC INFORMATION AND INFORMATION SYSTEMS

In general, individual agencies should identify the mission information types processed by their systems. This Appendix identifies some sample information types that might be processed by Federal government organizations. Note that the material is provided as an example of mission information and potential impacts of unauthorized disclosure, modification, or unavailability of mission information. It is meant to be neither prescriptive nor part of the basic guideline.

The primary purpose for Federal government information systems is to support provision of basic services to U.S. citizens and residents. This section addresses information types associated with both services provided by the Federal government to citizens and mechanisms used to achieve the purposes of government or deliver services for citizens. Delivery mechanisms include financial vehicles, direct government delivery, and indirect government delivery. One hundred Federal government missions or delivery mechanisms distributed among twenty-five mission areas and modes of delivery are identified below. Each mission area and delivery mode corresponds to a *Services to Citizens* or *Mode of Delivery* business area as defined in the *Business Reference Model 2.0*. There is not a one-to-one mapping of services and delivery modes to government departments and agencies. Some departments and agencies focus on a single mission. Others support multiple missions within a mission area. Still others provide services associated with several different mission *areas***.**

An information type is associated with each Federal government mission and delivery mode. The identity of each information type is defined by the mission with which it is associated.

The common impact determination factors described in the introduction to Appendix C also apply to agency-specific information.

Table 4 is a list of the types of Federal government information treated in this section. The list and subsequent descriptive information conform to the missions activities and functions identified in the Office of Management and Budget's Federal Enterprise Architecture Program Management Office's *Business Reference Model 2.0*.

Table 5 provides examples of possible impact assessments for each potential mission information type or delivery mode represented in Table 4.

The following sections describe information attributes that drive and/or affect impact assessment for each information type.

Table 4: Mission Information Types and Delivery Mechanisms		
Mission Areas and Information Types		
Defense & National Security	***Economic Development***	***Income Security***
Homeland Security	Business and Industry Development	General Retirement and Disability
Border & Transportation Security	Intellectual Property Protection	Unemployment Compensation
Key Asset & Critical Infrastructure Protection	Financial Sector Oversight	Housing Assistance
Catastrophic Defense	Industry Sector Income Stabilization	Food & Nutrition Assistance
Intelligence	*Community & Social Services*	Survivor Compensation
Disaster Management	Homeownership Protection	***Law Enforcement***
Disaster Monitoring & Prediction	Community & Regional Development	Criminal Apprehension
Disaster Preparedness & Planning	Social Services	Criminal Investigation & Surveillance
Disaster Repair & Restoration	Postal Services	Citizen Protection
Emergency Response	***Transportation***	Crime Prevention
International Affairs & Commerce	Air Transportation	Leadership Protection
Foreign Affairs	Ground Transportation	Property Protection
Int'l Development & Humanitarian Aid	Water Transportation	Substance Control
Global Trade	Space Operations	***Litigation & Judicial Activities***
Natural Resources	***Education***	Judicial Hearings
Water Resource Management	Elementary, Secondary, & Vocational Ed	Legal Defense
Conservation, Land, & Marine Mgt	Higher Education	Legal Investigation
Recreational Resource Mgt & Tourism	Cultural & Historic Preservation	Legal Prosecution and Litigation
Agricultural Innovation & Services	Cultural & Historic Exhibition	Dispute Resolution Facilitation
Energy	***Workforce Management***	*Federal Correctional Activities*
Energy Supply	Training and Employment	Criminal Incarceration
Energy Conservation & Preparedness	Labor Rights Management	Criminal Rehabilitation
Energy Production	Worker Safety	***General Science & Innovation***
Energy Resource Management	***Health***	Scientific/Tech Research & Innovation
Environmental Management	Illness Prevention	Space Exploration & Innovation
Environmental Monitoring and Forecasting	Immunization Management	
Environmental Remediation	Public Health Monitoring	
Pollution Prevention & Control	Health Care Services	
	Consumer Health & Safety	
Modes of Delivery		
Services Delivery Mechanisms and Information Types		
Knowledge Creation & Management	***Regulatory Compliance & Enforcement***	***Public Goods Creation and Management***
General Purpose Data and Statistics	Inspections and Auditing	Manufacturing
Research and Development	Standards/Reporting Guideline Dev't	Construction
Advising and Consulting	Permits and Licensing	Public Resources, Facility & Infrastructure
Knowledge Dissemination		Information Infrastructure Management
Financial Vehicles and Information Types		
Federal Financial Assistance	***Credit and Insurance***	***Transfers to State/Local Governments***
Federal Grants (Non-State)	Direct Loans	Formula Grants
Direct Transfers to Individuals	Loan Guarantees	Project/Competitive Grants
Subsidies	General Insurance	Earmarked Grants
Tax Credits		State Loans

Table 5: Security Categorization of Mission Information			
	Confidentiality	Integrity	Availability
Defense & National Security	Nat'l Security	Nat'l Security	Nat'l Security
Homeland Security			
Border Control and Transportation Security	Moderate	Moderate	Moderate
Key Asset and Critical Infrastructure Protection	High	High	High
Catastrophic Defense	High	High	High
Intelligence Operations[10]	High	High	High
Disaster Management			
Disaster Monitoring and Prediction	Low	High	High
Disaster Preparedness and Planning	Low	Low	Low
Disaster Repair and Restoration	Low	Low	Low
Emergency Response	Low	High	High
International Affairs and Commerce			
Foreign Relations	High	High	Moderate
International Development and Humanitarian Aid	Moderate	Low	Low
Global Trade	High	High	High
Natural Resources			
Water Resource Management	Low	Low	Low
Conservation, Marine, and Land Management	Low	Low	Low
Recreational Resource Management and Tourism	Low	Low	Low
Agricultural Innovation and Services	Low	Low	Low
Energy			
Energy Supply	Low[11]	Low[12]	Low[15]
Energy Conservation and Preparedness	Low	Low	Low
Energy Resource Management	Moderate	Low	Low
Energy Production	Low	Low	Low
Environmental Management			
Environmental Monitoring and Forecasting	Low	Moderate	Low
Environmental Remediation	Moderate	Low	Low
Pollution Prevention And Control	Low	Low	Low
Economic Development			
Business and Industry Development	Low	Low	Low
Intellectual Property Protection	Low	Low	Low
Financial Sector Oversight	Moderate	Low	Low
Industry Sector Income Stabilization	Moderate	Low	Low
Community and Social Services			
Homeowner Promotion	Low	Low	Low
Community and Regional Development	Low	Low	Low
Social Services	Low	Low	Low
Postal Services	Low	Moderate	Moderate

[10] Where foreign intelligence information is involved, the information and information systems are categorized as *national security* information or systems and are outside the scope of this guideline.
[11] High where safety of radioactive materials, highly flammable fuels, or transmissionchannels or control processes at risk.
[12] Usually Moderate or High where time-critical proccesses are involved.

Table 5 (Cont'd): Security Categorization of Mission Operations Information

	Confidentiality	Integrity	Availability
Transportation			
Ground Transportation	Low	Low	Low
Water Transportation	Low	Low	Low
Air Transportation	Low	High	High
Space Operations	Low	High	High
Education			
Elementary, Secondary, & Vocational Ed	Low	Low	Low
Higher Education	Low	Low	Low
Cultural & Historic Preservation	Low	Low	Low
Cultural & Historic Exhibition	Low	Low	Low
Workforce Management			
Training and Employment	Low	Low	Low
Labor Rights Management	Low	Low	Low
Worker Safety	Low	Low	Low
Public Health			
Illness Prevention	Low	Low	Low
Immunization Management	Low	Low	Low
Public Health Monitoring	Low	Low	Low
Health Care Services	Low	High	Low
Consumer Health and Safety	Low	Moderate	Low
Income Security			
General Retirement and Disability	Low	Low	Low
Unemployment Compensation	Low	Low	Low
Housing Assistance	Low	Low	Low
Food and Nutrition Assistance	Low	Low	Low
Survivor Compensation	Low	Low	Low
Law Enforcement			
Criminal Apprehension	High	Moderate	High
Criminal Investigation and Surveillance	High	Moderate	Moderate
Citizen Protection	Moderate	Moderate	High
Leadership Protection	High	High	High
Property Protection	Moderate	Moderate	Moderate
Substance Control	High	High	Low
Crime Prevention	Low	Low	Low
Trade Law Enforcement	High	High	High
Litigation and Judicial Activities			
Judicial Hearings	High	Low	Low
Legal Defense	High	High	Low
Legal Investigation	High	Moderate	Moderate
Legal Prosecution and Litigation	High	High	Low
Resolution Facilitation	High	Low	Low
Federal Correctional Activities			
Criminal Incarceration	Low	Moderate	Low
Criminal Rehabilitation	Low	Low	Low

Table 5 (Cont'd): Security Categorization of Mission Operations Information			
	Confidentiality	Integrity	Availability
General Science and Innovation			
Scientific & Tech Research & Innovation	Low	Moderate	Low
Space Exploration & Innovation	Low	Moderate	Low
Knowledge Creation and Management			
Research and Development	Low	Moderate	Low
General Purpose Data and Statistics	Low	Low	Low
Advising and Consulting	Low	Low	Low
Knowledge Dissemination	Low	Low	Low
Regulatory Compliance and Enforcement			
Inspections and Auditing	Moderate	Moderate	Low
Standard Setting/Reporting Guideline Dev't	Low	Low	Low
Permits and Licensing	Low	Low	Low
Public Goods Creation and Management			
Manufacturing	Low	Low	Low
Construction	Low	Low	Low
Public Facility and Infrastructure	Low	Low	Low
Information Infrastructure Management	Low	Low	Low
Federal Financial Assistance			
Federal Grants (Non-State)	Low	Low	Low
Direct Transfers to Individuals	Low	Low	Low
Subsidies	Low	Moderate	Low
Tax Credits	Moderate	Low	Low
Credits and Insurance			
Direct Loans	Low	Low	Low
Loan Guarantees	Low	Low	Low
General Insurance	Low	Low	Low
Transfers to State/Local Governments			
Formula Grants	Low	Low	Low
Project/Competitive Grants	Low	Low	Low
Earmarked Grants	Low	Low	Low
State Loans	Low	Low	Low

D.1 Defense and National Security

Defense and national security operations protect and advance U.S. National Security interests and, if deterrence fails, decisively defeat threats to those interests. Defense and national security activities include but are not limited to military operations, border protection, and intelligence gathering. Defense operations are subdivided into the following classes:

- **Strategic National and Theater Defense** – Establishing national and multinational military objectives, sequencing initiatives, defining limits and assessing risks for the use of military and other instruments of national power, developing global plans or theater war plans to achieve these objectives, and

providing military forces and other capabilities in accordance with strategic plans;

- **Operational Defense** – linking tactics and strategy by establishing operational objectives needed to accomplish the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events; and
- **Tactical Defense** – the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives.

Note that impacts to much information and many information systems associated with each defense and national security mission may affect the security of a broad range of critical infrastructures and key national assets. Systems the function, operation, or use of which, involve command and control of military forces, weapons control[13], involve equipment that is an integral part of a weapon or weapons system, are critical to the direct fulfillment of military missions[2] or are otherwise employed in strictly military operations[14] are defined under Public Law[7] as *national security systems.* Information assurance responsibilities are delegated to the Department of Defense for systems that are operated by the Department of Defense, or another entity on behalf of the Department of Defense that processes any information, the unauthorized use, disclosure, disruption, modification, or disruption of which would have a debilitating impact on the mission of the Department of Defense[15]. Security objectives and impact levels associated with these systems are determined by the Department of Defense.

D.2 Homeland Security

Homeland Security involves protecting the nation against terrorist attacks. This includes analyzing threats and intelligence, guarding borders and airports, protecting critical infrastructure, and coordinating the response emergencies. The Homeland Security Line of Business is defined by the President's Strategy on Homeland Security. Note: Some of the Critical Mission Areas from the President's strategy are included in other information classes and categories.

D.2.1 Border and Transportation Security Information Type

Border and Transportation Security includes appropriately facilitating or deterring entry and exit of people, goods, and conveyances at and between U.S. ports of entry, as well as ensuring the security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States. Border control involves enforcing the laws regulating the admission of foreign-born persons (i.e., aliens) to the United States. This involves the patrolling and monitoring of borders as well as deportation of illegal aliens.

---

[13] Weapons control involves the actions taken to monitor and protect U.S. weaponry, as well as the oversight and control of arms in other countries. Weapons Control applies to conventional, biological, chemical, and nuclear weaponry.

[14] Military operations involve the activities that take place during base trainings, military conflicts, and peacekeeping missions.

[15] *Federal Information Security Management Act of 2002*, Public Law 107-347, Subchapter III – Information Security, Sec. 3543(c)(2), 12/17/02.

Note that some border control information is also associated with other mission information types (e.g., criminal apprehension, and criminal investigation and surveillance information). In such cases, the impact levels of the associated mission information may determine impact levels associated with border control information. In some cases the border control information may be classified. Any classified information is treated under separate rules established for *national security information*. Note also that some aspects of ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States are also covered under the information types associated with the transportation mission. The recommended categorization for unclassified border and transportation security information follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, MODERATE)}

D.2.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of border control information on the ability of responsible agencies to enforce laws regulating the admission of foreign-born persons (i.e., aliens) to the United States. Where border control information is also associated with other mission information types (e.g., criminal apprehension, and criminal investigation and surveillance information), the confidentiality impact level associated with the information may be ***high***. Also, where unauthorized disclosure of border control information may be expected to put the physical safety of personnel into serious jeopardy, the confidentiality impact level associated with the information may be ***high***. Generally, however, the effects of unauthorized disclosure of border control information are usually confined to a single geographic region, immigration case, or deportation case. Even so, unauthorized disclosure may have a serious adverse effect on mission functions, cause significant degradation in mission capability, or place the agency at a significant disadvantage with respect to its border control responsibilities. Particularly in the case of immigration, naturalization, and deportation activities, unauthorized disclosure of information can violate privacy policies. Such unauthorized disclosures can have a serious effect on public confidence in the agency.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of confidentiality of information associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States can result in facilitation of terrorist activities that endanger human life. In some cases, the consequent threat to critical infrastructures, key national assets, and human life can be catastrophic. Consequently, the confidentiality impact level associated with information associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States is normally ***high***.

Recommended Confidentiality Impact Level: The default confidentiality level recommended for most border control information is ***moderate***.

D.2.1.2 Integrity

The consequences of unauthorized modification or destruction of border control information can generally be overcome if basic mitigating procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. The consequences of unauthorized modification or destruction of information can be serious or catastrophic if its nature and timing results in modification of information critical to tactical operations. The consequences can be equally serious if the destruction or modification of information renders ineffective confidentiality mechanisms that protect high-impact or moderate-impact information.

Special Factors Affecting Confidentiality Impact Determination: In the case of information associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States, mission requirements may not permit sufficient time to recognize anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives. Unauthorized modification or destruction of information affecting anti-terrorism information may adversely affect mission operations in a manner that results in unacceptable damage to critical infrastructures, damage to or loss of key national assets, or loss of human life. Consequently, the integrity impact level associated with information associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States is normally ***high***.

Recommended Integrity Impact Level: Subject to caveats regarding information shared with other mission types (e.g., anti-terrorism), the default integrity impact level recommended for border control information is ***moderate***.

D.2.1.3 Availability

The effects of disruption of access to or use of border control information or information systems can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. The nature of most border control processes is usually tolerant of delays. Alternate communications media and retention of copies of source material can generally prevent significant degradation in mission capability and major damage to assets that require extensive corrective action or repairs.

Special Factors Affecting Availability Impact Determination: There may be time critical cases. Examples include communication of information regarding transport of illegal aliens under conditions that threaten the lives of the aliens, communicating to border control points the undesirable status of individuals attempting to enter the country, or a physical threat posed by aliens that border control personnel have been assigned to interdict. In such cased, the availability impact can be ***high***. Except for

such time-critical cases, cases where impact is driven by information shared with associated missions (e.g., anti-terrorism), the availability impact level recommended for border control information is normally ***moderate***.

Special Factors Affecting Availability Impact Determination: The effects of disruption of access to or use of information or information systems associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States cannot necessarily be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of anti-terrorism missions is not reliably tolerant of delays. Alternate communications media and retention of copies of source material cannot be depended on to prevent significant degradation in mission capability and resultant catastrophic consequences for critical infrastructures, key national assets, and/or human life. In general, the availability impact level associated with information or information systems associated with ensuring security of transportation and infrastructure networks, facilities, vehicles, and personnel within the United States is ***high***.

Recommended Availability Impact Level: The default availability impact level associated with border control information is ***moderate***.

D.2.2 Key Asset and Critical Infrastructure Protection Information Type

Key Asset and Critical Infrastructure Protection involves assessing key asset and critical infrastructure vulnerabilities and taking direct action to mitigate vulnerabilities, enhance security, and ensure continuity and necessary redundancy in government operations and personnel. Under the provisions of Executive Order 13292, some anti-terrorism information is subject to security classification. This classified information is treated under separate rules established for *national security information*. The recommended categorization for unclassified anti-terrorism information follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, HIGH), (**availability**, HIGH)}

D.2.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of critical infrastructure protection information on the ability of responsible agencies to monitor and assess the leadership, motivations, plans, and intentions of foreign and domestic terrorist groups and their state and non-state sponsors. The effects of unauthorized disclosure of this information can reasonably be expected to jeopardize fulfillment of critical infrastructure protection missions. The consequent threat to critical infrastructures, key national assets, and human life can be catastrophic.

Recommended Confidentiality Impact Level: The confidentiality impact level associated with critical infrastructure protection information is normally ***high***.

D.2.2.2 Integrity

The consequences of unauthorized modification or destruction of critical infrastructure protection information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. Mission requirements may not permit sufficient time to recognize anomalous information and compare suspect information to that contained in source materials. Unauthorized modification or destruction of information affecting critical infrastructure protection operations may adversely affect mission operations in a manner that results in unacceptable damage to critical infrastructures, damage to or loss of key national assets, or loss of human life.

Recommended Integrity Impact Level: The default integrity impact level recommended for critical infrastructure protection information is normally ***high***.

D.2.2.3 Availability

The effects of disruption of access to or use of critical infrastructure protection information or information systems cannot necessarily be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of critical infrastructure protection missions is not reliably tolerant of delays. Basic procedures and controls, such as alternate communications media and retention of copies of source material, cannot be depended on to prevent significant degradation in mission capability and resultant catastrophic consequences for critical infrastructures, key national assets, and/or human life.

Recommended Availability Impact Level: The default availability impact level recommended for critical infrastructure protection control information is ***high***.

D.2.3 Catastrophic Defense Information Type

Catastrophic Defense involves the development of technological countermeasures (chemical, biological, radiological and nuclear [CBRN]) to terrorist threats, conducting laboratory testing on new and promising devices, and conducting basic and applied science that can lead to the development of countermeasures. Under the provisions of Executive Order 13292, some anti-terrorism information is subject to security classification. This classified information is treated under separate rules established for *national security information*. The recommended categorization for unclassified anti-terrorism information follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, HIGH), (**availability**, HIGH)}

D.2.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of catastrophic defense information on the ability of responsible agencies to monitor and assess the leadership, motivations, plans, and intentions of foreign and domestic terrorist groups and their state and non-state sponsors. The effects of unauthorized disclosure of this information can reasonably be expected to jeopardize fulfillment of catastrophic defense

missions. The consequent threat to human life, critical infrastructures, and key national assets can be catastrophic.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for catastrophic defense information is normally ***high***.

D.2.3.2 Integrity

The consequences of unauthorized modification or destruction of catastrophic defense information depends, not only on mitigating procedures and controls, but also on the urgency with which the antiterrorism information is needed. Mission requirements may not permit sufficient time to recognize anomalous information and compare suspect information to that contained in source materials. Unauthorized modification or destruction of information affecting catastrophic defense activities may adversely affect mission operations in a manner that results in loss of human life, unacceptable damage to critical infrastructures, and/or damage to or loss of key national assets.

Recommended Integrity Impact Level: The default integrity impact level recommended for catastrophic defense information is normally ***high***.

D.2.3.3 Availability

The effects of disruption of access to or use of catastrophic defense information or information systems cannot necessarily be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of catastrophic defense missions is not reliably tolerant of delays. Alternate communications media and retention of copies of source material cannot be depended on to prevent significant degradation in mission capability and resultant catastrophic consequences for human life, critical infrastructures, and/or key national assets.

Recommended Availability Impact Level: The default availability impact level recommended for catastrophic defense information is ***high***.

D.3 Intelligence Operations

Intelligence operations involve the development and management of accurate, comprehensive, and timely foreign intelligence on national security topics. Systems the function, operation, or use of which, involve intelligence activities or are critical to the direct fulfillment of intelligence missions[16] are defined under Public Law[17] as

[16] Systems that do not involve a) intelligence activities, b) cryptologic activities related to national security, c) command and control of military forces, d) equipment that is an integral part of a weapon or weapons system or 5) information classified by an act of Congress or under an Executive order are not designated as *national security systems* if they are used exclusively for routine business or administrative applications even if they are critical to the direct fulfillment of military or intelligence missions. Routine business or administrative applications are defined as including payroll, finance, logistics, and personnel management applications. [*Federal Information Security Management Act of 2002*, Public Law 107-347, Subchapter III – Information Security, Sec. 3547 – National security systems, 12/17/02]

national security systems. National security information and *national security systems* are, by definition, outside the scope of this guideline. Security objectives and impact levels associated with *national security systems* are determined by the head of each agency exercising control of the system[18].

Note that some agencies are charged with gathering ***domestic*** intelligence. Much domestic intelligence information is classified. Other domestic intelligence information may not be classified (e.g., some information obtained from state and local government sources). All classified information is treated under separate rules established for *national security information*. The recommended categorization for unclassified domestic intelligence information follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, HIGH), (**availability**, HIGH)}

D.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of domestic intelligence information on the ability of responsible agencies to develop and manage accurate, comprehensive, and timely domestic intelligence on homeland security topics and other *national* threats, but also with the use to which the information is put (e.g., threat warning, interdiction, criminal prosecution). The consequences of unauthorized disclosure of domestic intelligence information may include loss of the ability and/or authorization to collect information necessary to provide warning of or interdiction of major threats (e.g., terrorist threats to critical infrastructures and/or key national assets).

Recommended Confidentiality Impact Level: Given the criticality of much domestic intelligence information and the severe or catastrophic consequences to agencies that disclose domestic intelligence information without proper authorization (e.g., Privacy Act provisions, Fourth Amendment issues), the default confidentiality impact level recommended for the information is ***high***.

D.3.2 Integrity

Domestic intelligence information is generally associated with other mission-related information (e.g., anti-terrorism, firearms and explosive protection, narcotics interdiction). The consequences of unauthorized modification or destruction of domestic intelligence information is determined to a large extent on the missions being supported by the intelligence information. Also, the consequences of unauthorized modification or destruction of domestic intelligence information generally depends less on the adequacy of mitigating procedures and controls than on the urgency with which the intelligence information is needed. Mission requirements (e.g, threat warning or interdiction) may

---

[17] Clinger-Cohen Act, Public Law 104-106, *National Defense Authorization Act For Fiscal Year 1996*, Division E – Information Technology Reform, Sec. 5142 – National Security Systems Defined, 8/8/96; *Homeland Security Act of 2002*, Public Law 107-296, Title X – Information Security, Subchapter II, Sec. 3532 – Definitions, 11/25/02; and *Federal Information Security Management Act of 2002*, Public Law 107-347, Subchapter III – Information Security, Sec. 3542 – Definitions, 12/17/02.

[18] *Federal Information Security Management Act of 2002*, Public Law 107-347, Subchapter III – Information Security, Sec. 3547 – National security systems, 12/17/02.

not permit sufficient time to recognize anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives. Unauthorized modification or destruction of information affecting intelligence information may adversely affect mission operations in a manner that results in unacceptable damage to critical infrastructures, damage to or loss of key national assets, or loss of human life.

Recommended Integrity Impact Level: The default integrity impact level recommended for domestic intelligence information is normally ***high***.

D.3.3 Availability

The effects of disruption of access to or use of domestic intelligence information or information systems cannot necessarily be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of missions supported by domestic intelligence information is not reliably tolerant of delays. Basic procedures and controls, such as alternate communications media and retention of copies of source material, cannot be depended on to prevent significant degradation in mission capability and resultant catastrophic consequences for critical infrastructures, key national assets, and/or human life.

Recommended Availability Impact Level: The default availability impact level recommended for domestic intelligence information is ***high***.

D.4 Disaster Management

Disaster management involves the activities required to prepare for, mitigate, respond to, and repair the effects of all disasters whether natural or man-made. Note that compromise of much information associated with and many information systems supporting any of the missions within the disaster management mission area may seriously impact the security of a broad range of critical infrastructures and key national assets.

D.4.1 Disaster Monitoring and Prediction Information Type

Disaster monitoring and prediction involves the actions taken to predict when and where a disaster may take place and communicate that information to affected parties. The recommended baseline categorization of the disaster monitoring and protection information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, HIGH), (**availability**, HIGH)}

D.4.1.1 Confidentiality

The confidentiality impact level is effect of unauthorized disclosure of disaster monitoring and prediction information on the ability of responsible agencies to predict when and where a disaster may take place and communicate that information to affected parties. The purpose of disaster monitoring and prediction activities is generally to

disseminate information, not to conceal the information. Sharing of raw information by a diverse group of analysts often improves the quality of predictive analysis.

Special Factors Affecting Confidentiality Impact Determination: The consequences of unauthorized disclosure of some disaster monitoring and prediction information may include causing public panic or other responses that directly or indirectly jeopardize public safety, disaster prevention, emergency response, disaster repair, or restoration missions. For example, attempts of large populations to evacuate an endangered area before necessary preparations are made with respect to the evacuation routes can result in a clogging of the routes and failure to evacuate large parts of the population in time to save them from a life-threatening event. Given the criticality that much disaster monitoring and prediction information has in terms of potential loss of human life and major property damage, where unauthorized release of information can reasonably be expected to precipitate interference with disaster prevention or emergency response missions, the confidentiality impact level associated with the type information cited in the example can be ***moderate*** or ***high***. The unauthorized disclosure of disaster monitoring and prediction information to terrorists can, in some cases, reveal weak or sensitive points to target, the most effective technique(s) or approach(es) to use in attacking a target, and/or assumptions on the part of defensive organizations regarding the status, intent, and plans of our adversaries. Where unauthorized disclosure of disaster monitoring and prediction information is expected to be of direct use to terrorists, the confidentiality impact level is assumed to be ***high***.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for most disaster monitoring and prediction information is ***low***.

D.4.1.2 Integrity

The consequences of unauthorized modification to or destruction of disaster monitoring and prediction information usually depends on the urgency with which the information is needed. Mission requirements may not permit sufficient time to recognize anomalous information and compare suspect information to that contained in source materials. Unauthorized modification or destruction of information affecting disaster monitoring and prediction information may jeopardize public safety, disaster prevention, and/or emergency response missions in a manner that results in unacceptable damage to critical infrastructures, damage to or loss of key national assets, or loss of human life.

Recommended Integrity Impact Level: The default integrity impact level recommended for disaster monitoring and prediction information is normally ***high***.

D.4.1.3 Availability

The effects of disruption of access to or use of disaster monitoring and prediction information or information systems cannot necessarily be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of missions supported by disaster monitoring and prediction information is not reliably tolerant of delays. Delays measured in minutes can cost lives and irreplaceable property. Alternate communications media

and retention of copies of source material cannot be depended on to prevent significant degradation in mission capability and resultant catastrophic consequences for critical infrastructures, key national assets, and/or human life.

Recommended Availability Impact Level: The default availability impact level recommended for disaster monitoring and prediction information is ***high***.

D.4.2 Disaster Preparedness and Planning Information Type

Disaster preparedness and planning involves the development of response programs to be used in case of a disaster. This involves the development of emergency management programs and activities as well as staffing and equipping regional response centers. The recommended baseline categorization of the disaster preparedness and planning information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.4.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of disaster preparedness and planning information on the ability of responsible agencies to develop response programs to be used in case of a disaster. This involves the development of emergency management programs and activities as well as staffing and equipping regional response centers. The consequences of unauthorized disclosure of most disaster preparedness and planning information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: The consequences of unauthorized disclosure of some disaster preparedness and planning information may include revealing weak or sensitive critical infrastructure characteristics or inadequate security attributes of U.S. targets to terrorists or other adversaries. Such information may reveal to an enemy the most effective technique(s) or approach(es) to use in attacking a target, and/or assumptions on the part of defensive organizations regarding the capabilities, intent, and plans of our adversaries. Where unauthorized disclosure of disaster preparedness and planning information associated with critical infrastructures, large groups of people, or key national assets is expected to be of direct use to terrorists, the confidentiality impact level is assumed to be ***high***.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for most disaster preparedness and planning information is ***low***.

D.4.2.2 Integrity

The consequences of unauthorized modification to or destruction of disaster preparedness and planning information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. The consequences of unauthorized modification or destruction of disaster preparedness and planning information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous

information and compare suspect information to that contained in source material, back-up files, and/or archives.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. The consequences of unauthorized modification or destruction of information can be serious or catastrophic if its nature and timing results in modification of time-critical operational information. The consequences can be equally serious if the destruction or modification of information renders ineffective confidentiality mechanisms that protect high-impact information. In such cases, the impact level assigned would be ***moderate*** or ***high***.

Recommended Integrity Impact Level: The default integrity impact level associated with most disaster preparedness and planning information is ***low***.

D.4.2.3 Availability

The effects of disruption of access to or use of disaster preparedness and planning information or information systems cannot necessarily be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of missions supported by disaster preparedness and planning information is not reliably tolerant of delays. The consequences of inability of emergency responders and those responsible for repair and restoration activities to access preparedness and planning information in the event of an actual emergency can include confusion and delays. Basic procedures and controls, such as alternate communications media and retention of copies of source materials, cannot be depended on to prevent significant degradation in mission capability and resultant catastrophic consequences for critical infrastructures, key national assets, and/or human life. [Note that, on the other hand, adequate training in implementation of disaster plans can greatly mitigate the effects of disruption of access to the plans.]

Recommended Availability Impact Level: In general, given an adequate training regimen and/or availability of back-up plans, the default availability impact level recommended for disaster preparedness and planning information is ***low***.

D.4.3 Disaster Repair and Restoration Information Type

Disaster repair and restoration involves the cleanup and restoration activities that take place after a disaster. This involves the cleanup and rebuilding of any homes, buildings, roads, environmental resources, or infrastructure that may be damaged due to a disaster. The recommended baseline categorization of the disaster repair and restoration information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.4.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of disaster repair and restoration information on the ability of responsible agencies to conduct cleanup and restoration activities that take place after a disaster. This involves the cleanup and rebuilding of any homes, buildings, roads, environmental resources, or infrastructure that may be damaged due to a disaster. The consequences of unauthorized disclosure of most disaster repair and restoration information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for disaster repair and restoration information is ***low***.

D.4.3.2 Integrity

The consequences of unauthorized modification to or destruction of disaster repair and restoration information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. The consequences of unauthorized modification or destruction of disaster repair and restoration information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most disaster repair and restoration information is ***low***.

D.4.3.3 Availability

The effects of disruption of access to or use of disaster repair and restoration information or information systems can usually be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, and the nature of missions supported by disaster repair and restoration information is generally tolerant of delay. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can usually be depended on to prevent significant degradation in mission capability and resultant serious or catastrophic consequences.

Recommended Availability Impact Level: The default availability impact level recommended for disaster repair and restoration information is ***low***.

D.4.4 Emergency Response Information Type

Emergency Response involves the immediate actions taken to respond to a disaster. These actions include, but are not limited to, providing mobile telecommunications,

operational support, power generation, search and rescue, and medical life saving actions. Note that impacts to emergency response information and the information systems that process and store emergency response information could result in negative impacts on cross-jurisdictional coordination within the critical emergency services infrastructure and the general effectiveness of organizations tasked with emergency response missions. The recommended baseline categorization of the emergency response information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, HIGH), (**availability**, HIGH)}

D.4.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of emergency response information on the ability of responsible agencies to respond to a disaster. These actions include, but are not limited to, providing mobile telecommunications, operational support, power generation, search and rescue, and medical life saving actions. The consequences of unauthorized disclosure of emergency response information will usually have little or no adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In cases where an attack remains underway, unauthorized disclosure of emergency response information can provide information that might permit terrorists or other adversaries to target emergency response assets, thus jeopardizing emergency response personnel and materiel, public safety, and emergency response missions. Given the criticality that much emergency response information has in terms of potential loss of human life and major property damage, where unauthorized release of information can reasonably be expected to facilitate interference with emergency response missions, the confidentiality impact level can be ***moderate*** or ***high***. Also, either anticipated or realized unauthorized disclosure of one agency's emergency response by another agency could result in negative impacts on cross-jurisdictional coordination within the critical emergency services infrastructure and the general effectiveness of organizations tasked with emergency response missions.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for emergency response information is ***low***.

D.4.4.2 Integrity

The consequences of unauthorized modification to or destruction of emergency response information usually depends on the urgency with which the information is needed. Mission requirements may not permit sufficient time to recognize anomalous information and compare suspect information to that contained in source materials. Unauthorized modification or destruction of information affecting emergency response information may pose a significant threat to major assets and/or human life.

Recommended Integrity Impact Level: The default integrity impact level recommended for emergency response information is normally ***high***.

D.4.4.3 Availability

The effects of disruption of access to or use of emergency response information or information systems cannot be expected to be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of missions supported by emergency response information is not tolerant of delays. Delays measured in minutes can cost lives and major property damage. Basic procedures and controls, such as alternate communications media and retention of copies of source material, cannot always be depended upon to prevent significant degradation in mission capability and resultant catastrophic consequences for critical infrastructures, key national assets, and/or human life.

Recommended Availability Impact Level: The default availability impact level recommended for emergency response information is ***high***.

D.5 International Affairs and Commerce

International Affairs and Commerce involves the non-military activities that promote U.S. policies and interests beyond our national borders, including the negotiation of conflict resolution, treaties, and agreements. In addition, this function includes: foreign economic development and social/political development; diplomatic relations with other Nations; humanitarian, technical and other developmental assistance to key Nations; and global trade. Note that information processed in or by systems operated by an agency or by the contractor of an agency that is protected at all times by procedures established and specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interests of foreign policy is *national security related*[19]. Security objectives and impact levels associated with such *national security information* are determined by the head of each agency exercising control of the system[6] and are outside the scope of this guideline.

D.5.1 Foreign Relations Information Type

Foreign Affairs refers to those activities associated with the implementation of foreign policy and diplomatic relations, including the operation of embassies, consulates, and other posts; ongoing membership in international organizations; the development of cooperative frameworks to improve relations with other Nations; and the development of treaties and agreements. Conflict resolution involves the mitigation and prevention of disputes stemming from inter and intra-state disagreements. Some conflict resolution information is subject to security classification. This classified information is treated under separate rules established for *national security information*. Treaties and agreements involves the negotiation and implementation of accords with foreign governments and organizations in efforts related to arms reduction and regulation, trade matters, criminal investigations and extraditions, and other various types of foreign policy. Note that where treaties and agreements information affects intelligence gathering and/or law enforcement cooperation, impacts to such information and the

[19] *Federal Information Security Management Act of 2002*, Public Law 107-347, Subchapter III – Information Security, Sec. 3542(b)(2)(A)(ii), 12/17/02.

information systems that process and store the information could result in negative impacts on protection of a broad range of critical infrastructures and key national assets. Some information associated with treaties and agreements is subject to security classification. This classified information is treated under separate rules established for *national security information*. The recommended categorization for unclassified foreign relations information follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, HIGH), (**availability**, MODERATE)}

D.5.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of conflict resolution information on the ability of responsible agencies to mitigate and prevent disputes stemming from inter and intra-state disagreements. Unauthorized disclosure of conflict information can reasonably be expected to jeopardize fulfillment of conflict resolution missions. This is particularly true of premature exposure of resolution factors, assumptions concerning motivations and personalities, and proposed solutions to adversaries. Some information that has supported a conflict resolution process can even undo the results of successful conflict resolution processes. The consequent threat to public confidence in the agency can cause a catastrophic adverse effect on an agency's mission capability. Where information includes candid opinions of agency personnel, or involvement of agency personnel in specific prior activities, the effectiveness of those personnel for many future agency missions can be permanently impaired. The consequences of failed conflict resolution activities often pose threats to human life and major property assets – sometimes on a massive scale. Consequently, the general confidentiality impact level associated with conflict resolution information is ***high***.

Special Factors Affecting Confidentiality Impact Determination: The level of confidentiality impact assigned to information associated with treaties and agreements is generally affected by its effect on the ability of responsible agencies to negotiate and implement accords with foreign governments and organizations in efforts related to arms reduction and regulation, trade matters, criminal investigations and extraditions, and other various types of foreign policy. Unauthorized disclosure of information associated with treaties and agreements can reasonably be expected to prevent successful negotiation and/or ratification of the treaties and agreements. This is particularly true of prematurely exposing of resolution factors, assumptions concerning motivations and personalities, and proposed solutions to adversaries. Some information that has supported a treaty or other international agreement process can even undo the results of successfully completed treaty or agreement. The consequent threat to public confidence in the agency can cause a catastrophic adverse effect on an agency's mission capability. Where information includes candid opinions of agency personnel, or involvement of agency personnel in specific prior activities, the effectiveness of those personnel for many future agency missions can be permanently impaired. The consequences of failure to successfully conclude treaties and other international agreements often pose threats to human life and major property assets – sometimes on a massive scale.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for information associated with treaties and agreements is ***high***.

D.5.1.2 Integrity

The consequences of unauthorized modification or destruction of conflict resolution information depend, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. Mission requirements may not permit sufficient time to recognize anomalous information and compare suspect information to that contained in source materials before the information is used in negotiations or other operations. Unauthorized modification or destruction of information affecting conflict resolution information may adversely affect mission operations in a manner that results in unacceptable consequences in terms of loss of human life and/or major property assets. Consequently, the default integrity impact level associated with conflict resolution information is ***high***. The consequences of unauthorized modification or destruction of information associated with treaties and agreements also depend, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. The consequences of unauthorized modification or destruction of information associated with treaties and agreements can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. The consequences of unauthorized modification or destruction of information can be serious or catastrophic if its nature and timing results in modification of time-critical operational information. The consequences can be equally serious if the destruction or modification of information renders ineffective confidentiality mechanisms that protect high-impact information. In such cases, the impact level assigned would be ***high***. However, the default integrity impact level associated with most information associated with treaties and agreements is ***low***.

Recommended Integrity Impact Level: Based on the criticality of conflict resolution information the default integrity impact level recommended for foreign relations information is ***high***.

D.5.1.3 Availability

The effects of disruption of access to or use of conflict resolution information or information systems can often be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of conflict resolution missions is often tolerant of significant delays. Where this is not the case, the availability impact associated with conflict resolution information may be ***high***. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can prevent significant degradation in mission capability and resultant catastrophic mission failures with attendant consequences for major assets and/or human life. In general,

the availability impact level associated with conflict resolution information is ***moderate***.

Special Factors Affecting Availability Impact Determination: The effects of disruption of access to or use of information or information systems associated with treaties and agreements can often be repaired in time to prevent catastrophic loss. As in other cases, the time frame required for repair is dependent on mitigating procedures and controls, but the nature of diplomatic missions is often tolerant of delays. Where this is not the case, the availability impact assigned with information associated with treaties and agreements may be ***high***. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can prevent significant degradation in mission capability and resultant catastrophic mission failures with attendant consequences for major assets and/or human life. In general, the availability impact level assigned to information associated with treaties and agreements is ***low***.

Recommended Availability Impact Level: Given the availability impact level associated with conflict resolution information, the default availability impact level recommended for foreign relations information is ***moderate***.

D.5.2 International Development and Humanitarian Aid Information Type

International Development and Humanitarian Aid refers to those activities related to the implementation of development and humanitarian assistance programs to developing and transitioning countries throughout the world. Development and aid may include technical assistance (the transfer of knowledge and expertise), and the delivery of equipment, commodities and urgent humanitarian assistance including food aid. In some cases, international development and humanitarian aid information is subject to security classification. This classified information is treated under separate rules established for *national security information*. The recommended categorization for unclassified international development and humanitarian aid information follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

D.5.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of international development and humanitarian aid information on the ability of responsible agencies to execute programs relating to debt relief, foreign investments, poverty alleviation and food relief, foreign market expansion, and donations, as well as the establishment of policies and procedures to facilitate economic development. Unauthorized disclosure of international development and humanitarian aid information may not directly jeopardize foreign socio-economic and political development missions, but the secondary effects of premature disclosure of this information may adversely affect agency credibility or give unfair competitive advantages to candidates for mission support activities (hence, increase mission costs and damage public confidence in the agency). These secondary effects can have a destabilizing effect on the intended beneficiaries and can result, in extreme cases, in threats to human life, major assets, or even ability of the agency to

effectively perform future missions. Some information that has supported an international development and humanitarian aid process can even undo the results of successfully completed foreign socio-economic and political development processes. The consequences of failed foreign socio-economic and political development activities may not often pose threats to human life and major property assets, but such threats can sometimes be realized on a massive scale. Where there is a possibility of such catastrophic consequences, a ***high*** confidentiality impact level must be assigned.

Recommended Confidentiality Impact Level: In general, the default confidentiality impact level recommended for international development and humanitarian aid information is ***moderate***.

D.5.2.2 Integrity

The consequences of unauthorized modification or destruction of international development and humanitarian aid information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. The consequences of unauthorized modification or destruction of international development and humanitarian aid information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. The consequences of unauthorized modification or destruction of information can be serious or catastrophic if its nature and timing results in modification of time-critical operational information. The consequences can be equally serious if the destruction or modification of information renders ineffective confidentiality mechanisms that protect high-impact or moderate-impact information. In such cases, the impact level assigned would be ***moderate*** or ***high***.

Recommended Integrity Impact Level: The default integrity impact level recommended for most international development and humanitarian aid information is ***low***.

D.5.2.3 Availability

The effects of disruption of access to or use of international development and humanitarian aid information or information systems can often be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of international development and humanitarian aid missions is often tolerant of delays. Where this is not the case, the availability impact associated with international development and humanitarian aid information may be ***moderate*** or ***high***. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can

prevent significant degradation in mission capability and resultant catastrophic mission failures with attendant consequences for major assets and/or human life.

Recommended Availability Impact Level: The default availability impact level recommended for international development and humanitarian aid information is ***low***.

D.5.3 Global Trade Information Type

Global Trade refers to those activities the Federal Government undertakes to advance worldwide economic prosperity by increasing trade through the opening of overseas markets and freeing the flow of goods, services, and capital. Trade encompasses all activities associated with the importing and exporting of goods to and from the United States. This includes goods declaration, fee payments, and delivery/shipment authorization. Export promotion involves the development of opportunities for the expansion of U.S. exports. Merchandise inspection refers to the verification of goods and merchandise as well as the surveillance, interdiction, and investigation of imports/exports in violation of various Customs laws. Tariffs/quotas monitoring refers to the monitoring and modification of the schedules of items imported and exported to and from the United States. The recommended categorization for the global trade information type follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, HIGH), (**availability**, HIGH)}

D.5.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of export promotion information on the ability of responsible agencies to mitigate and prevent disputes stemming from inter and intra-state disagreements. Unauthorized disclosure of trade agreement information can reasonably be expected to jeopardize fulfillment of export promotion missions. This is particularly true of premature exposure of trade agreement factors, assumptions concerning pricing, intentions and personalities, and proposed agreements. Some information that has supported an export promotion process can even undo the results of successful export promotion processes. The consequent threat to agency image or reputations can cause a catastrophic adverse effect on an agency's mission capability. Where information includes candid opinions of the participants, personnel involved in negotiations, or involvement of agency personnel in specific prior activities, the effectiveness of those personnel for future trade missions can be permanently impaired. Consequently, the general confidentiality risk level associated with export promotion information is ***high***. The confidentiality impact level is the effect of unauthorized disclosure of merchandise inspection information on the ability of responsible agencies to accurately determine, report, and record the discovered status of imported or exported merchandise as it bears on violations of various Customs laws. Unauthorized disclosure of merchandise inspection information cannot reasonably be expected to jeopardize fulfillment of other merchandise inspection missions, as the discovered status of shipments is generally information of public record. Some information that has supported a merchandise inspection process might be of higher sensitivity, such as cueing, tip-offs, and the like, and unauthorized disclosure of such might jeopardize the success of future merchandise inspection processes. The consequent threat to agency image or reputations can cause a serious adverse effect on an agency's

mission capability. Where information includes names of informants, personnel involved in informant contact, or involvement of agency personnel in specific prior activities, the effectiveness of those personnel for future inspection activities can be permanently impaired, or those individuals could potentially be exposed to personal hazard. Consequently, the general confidentiality risk level associated with merchandise inspection information is ***high***. The confidentiality impact level is the effect of unauthorized disclosure of tariffs/quotas monitoring information on the ability of responsible agencies to enforce various Customs laws, and preserve statistical data concerning the historical compliance with such laws. Unauthorized disclosure of tariffs/quotas monitoring information can not reasonably be expected to jeopardize fulfillment of other tariffs/quotas monitoring missions, as both the statutory tariffs/quotas, as well as the specifics of compliance therewith is public record.

Special Factors Affecting Confidentiality Impact Determination: Some information that has supported a tariffs/quotas monitoring process might be of higher sensitivity, such as targeting, intelligence information[20] which might point to a dumping situation, and the like, and unauthorized disclosure of such might jeopardize the success of future tariffs/quotas monitoring processes. In the case of intelligence information, this falls under *national security systems. National security information* and *national security systems* are, by definition, outside the scope of this guideline. The consequent threat to agency image or reputations can cause a serious adverse effect on an agency's mission capability. Where information includes names of informants, personnel involved in informant contact, or involvement of agency personnel in specific prior activities, the effectiveness of those personnel in support of future monitoring activities can be permanently impaired, or those individuals could potentially be exposed to personal hazard. Consequently, the general confidentiality risk level associated with tariffs/quotas monitoring information is ***high***.

Recommended Confidentiality Impact Level: The overall default confidentiality impact level recommended for global trade information is ***high***.

D.5.3.2 Integrity

The consequences of unauthorized modification or destruction of global trade information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. In the case of export promotion information, mission requirements will usually permit sufficient time to recognize anomalous information and compare suspect information to that contained in source materials before the information is used in negotiations or other operations. Unauthorized modification or destruction of information affecting export promotion information may adversely affect mission operations in a manner that results in unacceptable consequences in terms of potentially serious economic repercussions.

---

[20] Clinger-Cohen Act, Public Law 104-106, *National Defense Authorization Act For Fiscal Year 1996*, Division E – Information Technology Reform, Sec. 5142 – National Security Systems Defined, 8/8/96; *Homeland Security Act of 2002*, Public Law 107-296, Title X – Information Security, Subchapter II, Sec. 3532 – Definitions, 11/25/02; and *Federal Information Security Management Act of 2002*, Public Law 107-347, Subchapter III – Information Security, Sec. 3542 – Definitions, 12/17/02.

Additionally, once implemented, trade agreements are generally matters of public record, and thus the specifics of the negotiated terms, etc., are highly critical in terms of being accurately recorded. In the case of merchandise inspection, mission requirements generally do not permit sufficient time to recognize anomalous information and compare suspect information to that contained in source materials before the information is used, since such an occurrence could result in significant financial consequences to an importer or exporter whose shipment was in question. Unauthorized modification or destruction of information affecting merchandise inspection information may adversely affect mission operations in a manner that results in unacceptable consequences in terms of potentially serious economic repercussions. Additionally, once finalized, the results of inspections are matters of public record, and thus are highly critical in terms of being accurately recorded. In the case of tariffs/quotas monitoring information, the requirement for adequate means to detect data corruption is ***high***, since this information, particularly in long-term aggregation, is used in policy and strategic analysis, and accuracy of this statistical information is critical. Unauthorized modification or destruction of information affecting tariffs/quotas monitoring information may adversely affect mission operations in a manner that results in unacceptable consequences in terms of potentially catastrophic economic repercussions. Additionally, once finalized, the results of inspections are matters of public record, and thus are extremely critical in terms of being accurately recorded.

Recommended Integrity Impact Level: The default integrity risk level recommended for global trade information is ***high***.

D.5.3.3 Availability

The effects of disruption of access to or use of export promotion information or information systems can usually be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of export promotion missions is generally tolerant of significant delays. Where this is not the case, the availability risk associated with export promotion information may be ***high***. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can prevent significant degradation in fulfillment of the trade mission. In general, the availability risk level associated with export promotion information is ***moderate***.

Special Factors Affecting Availability Impact Determination: As in the case of export promotion information, the effects of disruption of access to or use of merchandise inspection information or information systems can often be repaired in time to prevent serious loss. The nature of merchandise inspection missions is also somewhat tolerant of significant delays. Where this is not the case, the availability risk associated with merchandise inspection information may be ***high***. This would be the case where such an occurrence could result in significant financial consequences where there was an uncertainty regarding the results of an importer's or exporter's shipment. In general, the default availability risk level associated with merchandise inspection information is ***high***. The nature of tariffs/quotas monitoring missions is also tolerant of significant delays. Mission requirements will almost invariably allow

sufficient time to restore access, rebuild files, and recognize anomalous information and compare suspect information to that contained in source material, back up files, and/or archives before the information is used. This information, particularly in long-term aggregation, is used in high level policy and strategic analysis, and lack of immediate access might cause an inconvenience but no significant mission impact. Even in this case, the availability risk associated with tariffs/quotas monitoring information may be ***high***, for instance if such an occurrence could result in serious damage to the image or reputation of an agency or even the national government, where there was an uncertainty regarding the compliance statistics of a major sovereign trade partner, etc.

Recommended Availability Impact Level: The default availability risk level recommended for global trade information is ***high***.

D.6 Natural Resources

The Natural Resources mission area includes all activities involved in conservation planning, land management, and national park/monument tourism that affect the nation's natural and recreational resources, both private and federal. Note: Energy-related natural resources are covered in the Energy Management mission area.

D.6.1 Water Resource Management Information Type

Water Resource Management includes all activities that promote the effective use and management of the nation's water resources. Notes: Environmental protection of water resources is included in the Environmental Management Line of Business. Hydroelectric energy production is included under the Energy Production mission. The recommended baseline categorization of the water resource management information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.6.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of water resource management information on the ability of responsible agencies to promote the effective use and management of the nation's water resources. The consequences of unauthorized disclosure of most water resource management information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: There may be some cases for which ***moderate*** confidentiality impact is associated with unauthorized disclosure of business/industry development. For example, unauthorized disclosure of details of current agency water resource management activities and plans can serve to focus opposition and/or give an unfair advantage to competing interests. Consistent premature disclosure of agency plans can cause significant degradation in mission capability.

Recommended Confidentiality Impact Level: As a rule, the default confidentiality impact recommended for business/industry development information is ***low***.

D.6.1.2 Integrity

The consequences of unauthorized modification to or destruction of water resource management information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. The consequences of unauthorized modification or destruction of water resource management information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications associated with water resource management information (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most water resource management information is ***low***.

D.6.1.3 Availability

The effects of disruption of access to or use of water resource management information or information systems can usually be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, and the nature of missions supported by water resource management information is generally tolerant of delay. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can usually be depended on to prevent significant degradation in mission capability and resultant serious or catastrophic consequences.

Recommended Availability Impact Level: The default availability impact level recommended for water resource management information is ***low***.

D.6.2 Conservation, Marine and Land Management Information Type

Conservation, Marine and Land Management involves the responsibilities of surveying, maintaining, and operating public lands and monuments, as well as activities devoted to ensuring the preservation of land, water, wildlife, and natural resources, both domestically and internationally. It also includes the sustainable stewardship of natural resources on federally owned/controlled lands for commercial use (mineral mining, grazing, forestry, fishing, etc.). The recommended baseline categorization of the conservation, marine, and land management information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.6.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of conservation, marine, and land management information on the ability of responsible agencies to survey, maintain, and operate public lands and monuments, as well as to ensure the preservation of land, water, wildlife, and natural resources, both domestically and internationally. The consequences of unauthorized disclosure of most conservation, marine, and land management information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: There may be some cases for which ***moderate*** confidentiality impact is associated with unauthorized disclosure of private or proprietary information associated with use of federally owned/controlled lands for commercial use (mineral mining, grazing, forestry, fishing, etc.). Additionally, unauthorized disclosure of details of current agency conservation, marine, and land management activities and plans can serve to focus opposition and/or give an unfair advantage to competing interests. Consistent premature disclosure of agency plans can cause significant degradation in mission capability. It is also noted that conservation, marine, and land management includes enforcement functions (e.g., the policing of marine fisheries). Confidentiality impacts associated with criminal apprehension, criminal investigation and surveillance, citizen protection, and property protection may cause the confidentiality impact of enforcement-related information to be ***moderate*** or ***high*** (see D.16).

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for most conservation, marine, and land management information is ***low***.

D.6.2.2 Integrity

The consequences of unauthorized modification to or destruction of conservation, marine, and land management information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. The consequences of unauthorized modification or destruction of conservation, marine, and land management information can generally be overcome if back-up and archiving procedures are adequate and are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications associated with conservation, marine, and land management information (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. Again, conservation, marine, and land management includes enforcement functions (e.g., the policing of marine fisheries). Integrity impacts associated with criminal apprehension, criminal investigation and surveillance, citizen protection, and property protection may cause the integrity impact of enforcement-related information to be ***moderate*** (see D.16).

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most conservation, marine, and land management information is ***low***.

D.6.2.3 Availability

The effects of disruption of access to or use of conservation, marine, and land management information or information systems can usually be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, and the nature of missions supported by conservation, marine, and land management information is generally tolerant of delay. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can usually be depended on to prevent significant degradation in mission capability and resultant serious or catastrophic consequences.

Special Factors Affecting Availability Impact Determination: Conservation, marine, and land management includes enforcement functions (e.g., the policing of marine fisheries). Availability impacts associated with criminal apprehension, criminal investigation and surveillance, citizen protection, and property protection may cause the confidentiality impact of enforcement-related information to be ***moderate*** or ***high*** (see D.16).

Recommended Availability Impact Level: The default availability impact level recommended for most conservation, marine, and land management information is ***low***.

D.6.3 Recreational Resource Management and Tourism Information Type

Recreational Resource Management and Tourism involves the management of national parks, monuments, and tourist attractions as well as visitor centers, campsites, and park service facilities. Note that impacts to some information and information systems associated with tourism management may affect the security of some key national assets (e.g., some national monuments and icons). The recommended baseline categorization of the recreational resource management and tourism information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.6.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of recreational resource management and tourism information on the ability of responsible agencies to manage of national parks, monuments, and tourist attractions as well as visitor centers, campsites, and park service facilities. The consequences of unauthorized disclosure of most recreational resource management and tourism information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: It is noted that recreational resource management and tourism includes enforcement functions (e.g.,

protective and enforcement functions of the National Park Service). Confidentiality impacts associated with criminal apprehension, criminal investigation and surveillance, citizen protection, and property protection may cause the confidentiality impact of enforcement-related information to be ***moderate*** or ***high*** (see D.16). The consequences unauthorized disclosure of details of property and tourist protection information can be particularly severe in the case of protection of national monuments and icons.

Recommended Confidentiality Impact Level: The confidentiality impact recommended for most recreational resource management and tourism information is ***low***.

D.6.3.2 Integrity

The consequences of unauthorized modification to or destruction of recreational resource management and tourism information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. The consequences of unauthorized modification or destruction of recreational resource management and tourism information can generally be overcome if back-up and archiving procedures are adequate and are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications associated with recreational resource management and tourism information (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. Again, recreational resource management and tourism includes enforcement functions (e.g., protective and enforcement functions of the National Park Service). Integrity impacts associated with criminal apprehension, criminal investigation and surveillance, citizen protection, and property protection may cause the integrity impact of enforcement-related information to be ***moderate*** or ***high*** (see D.16). For example, the requirements of protective activities may not permit sufficient time to recognize anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives (e.g., notices regarding suspected terrorists, outstanding criminal warrants). In such cases, protective measures can be jeopardized. Where terrorists or other criminals pose a threat to key national assets, or pose a threat to human life, the integrity impact level recommended for recreational resource management and tourism enforcement information is ***high***.

Recommended Integrity Impact Level: The default integrity impact level associated with modification or destruction of most recreational resource management and tourism information is ***low***.

D.6.3.3 Availability

The effects of disruption of access to or use of recreational resource management and tourism information or information systems can usually be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating

procedures and controls, and the nature of missions supported by recreational resource management and tourism information is generally tolerant of delay. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can usually be depended on to prevent significant degradation in mission capability and resultant serious or catastrophic consequences.

Special Factors Affecting Availability Impact Determination: Note that recreational resource management and tourism includes enforcement functions (e.g., protective and enforcement functions of the National Park Service). Availability impacts associated with criminal apprehension, criminal investigation and surveillance, citizen protection, and property protection may cause the confidentiality impact of enforcement-related information to be ***moderate*** or ***high*** (see D.16). There may also be time-critical cases associated with protection of people and key national assets from natural disasters (such as fires, unexpected blizzards, or volcanic eruptions). In such cased, the availability impact can be ***high***. Except for particularly time-critical cases, the availability impact level recommended for protection-related information is normally ***moderate***. The effects of disruption of access to or use of information or information systems associated with ensuring human safety and the safety of key national assets cannot necessarily be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on back-up and archiving facilities and procedures, but the nature of emergency notification and response (e.g., rescue) activities is not reliably tolerant of delays. Alternate communications media and retention of copies of source material cannot be depended on to prevent significant degradation in mission capability and resultant catastrophic consequences for key national assets and/or human life.

Recommended Availability Impact Level: Most recreational resource management and tourism information is routine in nature (not time-critical). Consequently, the default availability impact level recommended for most recreational resource management and tourism information is ***low***.

D.6.4 Agricultural Innovation and Services Information Type

Agricultural Innovation and Services involves the creation and dissemination of better methods for farming and the development of better and healthier crops. The recommended security categorization for the agricultural innovation and service information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.6.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of agricultural innovation and service information on the ability of responsible agencies to create and disseminate of better methods for farming and the development of better and healthier crops. In most cases, unauthorized disclosure of agricultural innovation and service information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In some cases, unauthorized disclosure of preliminary findings or policies under consideration regarding proposed agricultural products can result in unavailability of improved products, premature release of products that eventually prove to be dangerous, give an unfair advantage to particular commercial interests, and/or generate domestic or international public relations problems for the Federal government. In such cases, serious damage can result for agricultural innovation and service operations. Here, the confidentiality impact level may be ***moderate***. In other cases, unauthorized disclosure of information regarding creation, storage, and transportation of some particularly dangerous plant disease vectors, animal disease vectors, pesticides, and herbicides might facilitate malicious activities of terrorists or other criminals. Here, there is a potential for loss of human life, so the confidentiality impact level may be ***high***.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most agricultural innovation and service information is still ***low***.

D.6.4.2 Integrity

Agricultural innovation and service activities are not generally time-critical. The consequences of unauthorized modification of agricultural innovation and service information can generally be overcome if review procedures are in place and basic procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In most cases, the adverse effects of unauthorized modification to or destruction of agricultural innovation and service information on agency mission functions and public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for agricultural innovation and service information is ***low***.

D.6.4.3 Availability

The effects of disruption of access to or use of agricultural innovation and service information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Loan assistance processes are generally tolerant of delay. Availability and use of basic procedures and controls can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of agricultural innovation and service information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for agricultural innovation and service information is ***low***.

D.7 Energy

Energy refers to all actions performed by the government to ensure the procurement and management of energy resources, including the production, sale and distribution of

energy, as well as the management of spent fuel resources. Energy management includes all types of mass-produced energy (e.g., hydroelectric, nuclear, wind, solar, or fossil fuels). Also included in this mission area is the oversight of private industry.

D.7.1 Energy Supply Information Type

Energy Supply involves all activities devoted to ensuring the availability of an adequate supply of energy for the United States and its citizens. Energy Supply includes the sale and transportation of commodity fuels such as coal, oil, natural gas, and radioactive materials. This function also includes distributing and transferring power, electric generation, and/or storage located near the point of use. Note that impacts to some information and information systems associated with energy supply may affect the security of critical infrastructures, especially in the areas of energy transmission and transport. The following recommended baseline categorization of the energy supply information type is particularly subject to change where critical infrastructure elements or nuclear materials are involved:

SECURITY CATEGORY = {(**confidentiality**, LOW[21]), (**integrity**, LOW[18]), (**availability**, LOW[22])}

D.7.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of energy supply information on the ability of responsible agencies to conduct activities related to the sale and transportation of commodity fuels such as coal, oil, natural gas, and radioactive materials. This function also includes distributing and transferring power, electric generation, and/or storage located near the point of use.

Special Factors Affecting Confidentiality Impact Determination: The consequences of unauthorized and premature disclosure of energy supply information can have a serious economic impact with respect to competitive advantages and financial and commodity market dynamics. Even more seriously, unauthorized disclosure of supply information can assist terrorists (and simple thieves) in theft of energy products and materials or disruption of energy distribution channels. Facilitation of theft of nuclear materials is a particularly catastrophic potential result of unauthorized disclosure of specific types of energy supply information. In these cases, the confidentiality impact must be considered to be ***high***. [Note that some information regarding transportation and storage of nuclear materials is classified. The classified information is *national security related* and is outside the scope of this guideline. Other information, such as Nuclear Regulatory Commission "SAFEGUARDS" information is not *national security information*, but must be treated as having ***high*** confidentiality impact.] With respect to possible use by terrorists of energy distribution information regarding petroleum, natural gas, and other flammable or explosive products, a realistic impact assessment must take into account the wealth of non-Federal information that is susceptible to access by prospective perpetrators. Where distribution of hazardous energy products is involved, there is a potential unauthorized disclosure consequence of loss of human life and major property.

[21] Risk level is usually ***high*** where safety of radioactive materials, highly flammable fuels, or major transmission channels or control processes is at risk.
[22] Risk level is usually ***moderate*** or ***high*** where time-critical processes are involved.

In such cases the confidentiality impact level can be ***moderate*** or ***high***. [Note that disclosure of transportation routes and storage facilities is often (i) both authorized and necessary to mission accomplishment and (ii) authorized, or even mandated, for public safety reasons.] Also, either anticipated or realized unauthorized disclosure of one agency's energy supply information by another agency could result in negative impacts on cross-jurisdictional coordination within the energy distribution infrastructure and the general effectiveness of organizations tasked with energy supply.

Recommended Confidentiality Impact Level: In spite of the aforementioned cases where there is ***moderate*** or ***high*** impact associated with unauthorized disclosure of energy supply information, the default confidentiality impact level recommended for most energy supply information is ***low***.

D.7.1.2 Integrity

The consequences of unauthorized modification to or destruction of energy supply information usually depends on the urgency with which the information is needed or the immediacy with which the information is used. Undetected modification of automated switching functions in distribution channels (e.g., electrical power distribution, petroleum or gas pipelines) can result in loss of major assets or of human life. Consequently, the integrity impact level associated with these types of energy supply information used to control critical processes in real time is ***high***. The consequences of unauthorized modification to or destruction of less time-critical energy supply information can generally be overcome if basic mitigating procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most energy supply information is ***low***.

D.7.1.3 Availability

The effects of disruption of access to or use of energy supply information or information systems cannot always be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of functions supported by energy supply information is often not tolerant of delays. Delays measured in seconds can cost lives and major property damage. Basic procedures and controls, such as alternate communications media and retention of copies of source material, cannot always be depended upon to prevent significant degradation in mission capability and resultant serious or even catastrophic consequences for critical infrastructures, key national assets, and/or human life. In these cases, the availability impact level associated with energy supply information can be ***high***. The more common case is likely to be that disruption of access is sufficiently extensive to have a limited adverse effect on agency operations

(including mission, functions, or public confidence in the agency), agency assets, or individuals. In these cases, the availability impact level associated with energy supply information will be ***low***. Also, most energy supply information is not time-critical. Where the effects of disruption of access to or use of energy supply information or information systems can be expected to be repaired in time to prevent serious adverse effects, the availability impact level associated with energy supply information may be ***low***.

Recommended Availability Impact Level: In general, given implementation and use of basic procedures and controls, where processes to which the information is essential are either not time-critical or not likely to have serious or severe consequences, the availability impact level recommended for energy supply information is ***low***.

D.7.2 Energy Conservation and Preparedness Information Type

Energy Conservation and Preparedness involves protection of energy resources from over-consumption to ensure the continued availability of fuel resources and to promote environmental protection. This mission also includes measures taken to ensure the provision of energy in the event of an emergency. The recommended security categorization for the energy conservation and preparedness information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.7.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of energy conservation and preparedness information on the ability of responsible agencies to protect energy resources from over-consumption in order to ensure the continued availability of fuel resources and to promote environmental protection. In most cases, unauthorized disclosure of energy conservation and preparedness information will have only a limited adverse effect on agency operations, assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In some cases, unauthorized disclosure of preliminary findings or policies under consideration regarding proposed conservation measures or to permit efficient provisioning and distribution of energy in the event of an emergency can result in mobilization of special interests to successfully oppose necessary conservation measures, give an unfair advantage to particular commercial interests, and/or cause domestic or international loss of confidence in the Federal government. In such cases, serious damage can result for energy conservation and preparedness operations. Here, the confidentiality impact level may be ***moderate***. In other cases, unauthorized disclosure of information regarding measures taken to ensure the provision of energy in the event of an emergency facilitate malicious activities of terrorists. Here, there is a potential for loss of human life resulting from extended outages, so the confidentiality impact level may be ***high***.

Recommended Confidentiality Impact Level: The confidentiality impact level recommended for most energy conservation and preparedness information remains ***low***.

D.7.2.2 Integrity

Energy conservation and preparedness activities are not generally time-critical. The consequences of unauthorized modification or destruction of energy conservation and preparedness information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information necessary to time-critical processes ensuring the provision of energy in the event of an emergency can result in extended outages. There is some potential for a consequent threat to critical energy infrastructure and to human life. In such cases, the integrity impact level may be ***high***. However, in most cases, the adverse effects of unauthorized modification to or destruction of energy conservation and preparedness information on agency mission functions and public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for energy conservation and preparedness information is ***low***.

D.7.2.3 Availability

The effects of disruption of access to or use of energy conservation and preparedness information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls, facilities and procedures. Loan assistance processes are generally tolerant of delay. Availability and use of basic procedures and controls can usually prevent serious or catastrophic damage to mission capability.

Special Factors Affecting Availability Impact Determination: Unavailability of information necessary to time-critical processes ensuring the provision of energy in the event of an emergency can result in extended outages. There is some potential for a consequent threat to critical energy infrastructure and to human life. In such cases, the availability impact level may be ***high***. In most cases though, disruption of access to or use of energy conservation and preparedness information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for energy conservation and preparedness information is ***low***.

D.7.3 Energy Resource Management Information Type

Energy resource management involves the management of energy producing resources including facilities, land, and offshore resources. The recommended baseline categorization of the energy resource management information type follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

D.7.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of energy resource management information on the activities of responsible agencies with respect to management of energy producing resources including facilities, land, and offshore resources. Unauthorized disclosure of much energy resource management information can result in major financial consequences. In many cases, unauthorized disclosure of this information can impact financial markets and have a serious adverse effect on public confidence in the agency. Unauthorized disclosure of energy resource management information can create at least a ***moderate*** confidentiality impact. In some cases, the probable consequences of damage to public confidence in the agency can even be ***high***.

Recommended Confidentiality Impact Level: While the consequences of unauthorized disclosure of some energy resource management information would have only a limited adverse effect on agency operations, the consequences that can reasonably be expected to result from unauthorized disclosure of much energy resource management information justifies a ***moderate*** default confidentiality impact level.

D.7.3.2 Integrity

The consequences of unauthorized modification to or destruction of energy resource management information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is normally needed. The consequences of unauthorized modification or destruction of energy resource management information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. There may be on-line, automated, or semi-automated activities for which integrity threats can be realized before they are detected. Procedures are in place in most Federal energy resource management institutions to mitigate the effects of these consequences. Where unauthorized modification or destruction of energy resource management information facilitates or enables a serious or catastrophic confidentiality or availability impact scenario, the integrity impact level may be ***moderate*** or ***high***.

Recommended Integrity Impact Level: The default integrity impact level recommended for most modification or destruction of energy resource management information is ***low***.

D.7.3.3 Availability

The effects of disruption of access to or use of energy resource management information or information systems can usually be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, and the nature of missions supported by energy resource

management information is generally tolerant of delay. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can usually be depended on to prevent significant degradation in mission capability and resultant serious or catastrophic consequences.

Recommended Availability Impact Level: The default availability impact level recommended for energy resource management information is ***low***.

D.7.4 Energy Production Information Type

Energy production involves the transformation of raw energy resources into useable, deliverable energy. Note that impacts to some information and information systems associated with energy production may affect the security of the critical energy infrastructure. The recommended baseline categorization of the energy production information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.7.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of energy production information on the activities of responsible agencies with respect to transformation of raw energy resources into useable, deliverable energy. The consequences of unauthorized disclosure of most energy production information would have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some energy production information can result in major financial consequences. In some cases, premature disclosure of this information can impact financial markets. Unauthorized and premature disclosure to a single institution could damage faith in government institutions, result in adverse financial events, and have a serious adverse effect on public confidence in the agency. Unauthorized disclosure of energy production information can create at least a ***moderate*** confidentiality impact.

Recommended Confidentiality Impact Level: The probable consequences of unauthorized disclosure of most energy production information only justify a ***low*** default confidentiality impact level.

D.7.4.2 Integrity

The consequences of unauthorized modification to or destruction of energy production information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is normally needed. The consequences of unauthorized modification or destruction of energy production information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. There may be on-line, automated, or semi-automated activities for which integrity threats can be realized before they are detected. Where unauthorized modification or destruction of energy production information facilitates or enables a serious or catastrophic confidentiality or availability impact scenario, the integrity impact level may be ***moderate*** or ***high***.

Recommended Integrity Impact Level: The default integrity impact level recommended for most modification or destruction of energy production information is ***low***.

D.7.4.3 Availability

The effects of disruption of access to or use of energy production information or information systems can usually be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, and the nature of missions supported by energy production information is generally tolerant of delay. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can usually be depended on to prevent significant degradation in mission capability and resultant serious or catastrophic consequences.

Recommended Availability Impact Level: Except where the period of unavailability is long enough to shake the confidence of financial markets, the availability impact level recommended for energy production information is ***low***.

D.8 Environmental Management

Environmental management includes all functions required to determine proper environmental standards and ensure their compliance.

D.8.1 Environmental Monitoring and Forecasting Information Type

Environmental Monitoring and Forecasting involves the observation and prediction of environmental conditions. This includes but is not limited to the monitoring and forecasting of water quality, water levels, ice sheets, air quality, regulated and non-regulated emissions, as well as the observation and prediction of weather patterns and conditions. The following security categorization is recommended for the environmental monitoring and forecasting information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

D.8.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of environmental monitoring and forecasting information on the ability of responsible agencies to observe and predict environmental conditions. The consequences of unauthorized disclosure of most environmental monitoring information are unlikely to have a serious adverse effect

on agency operations. Due diligence with respect to legal procedures can mitigate these consequences.

Special Factors Affecting Confidentiality Impact Determination: The most serious adverse effects are likely to involve exposure of information that is proprietary to an organization being evaluated by the agency or can result in damaging publicity for an organization. [Note that unauthorized disclosure of some information can have serious economic impact on both individual companies and the broader market place (e.g., short-term stock market perturbations). The consequences of such unauthorized disclosures may have an adverse effect on public confidence in the agency, and may include short-term staffing challenges for the agency.] This is of particular concern where the data is preliminary and subject to error, misinterpretation, or change. In such cases, the potential confidentiality impacts can be at least ***moderate***.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most environmental monitoring and forecasting information is normally ***low***.

D.8.1.2 Integrity

The consequences of unauthorized modification or destruction of environmental monitoring information and forecasting can be serious if its nature and timing results in exposure of the public to harmful emissions, polluted water, etc. Unauthorized modification of environmental monitoring and forecasting information can also result in harm to both monitoring and monitored activities if altered data becomes public (a combination of realization of both integrity and confidentiality threats). In many cases, competent agency personnel should be able to recognize anomalous information (e.g., by recognizing information as suspect and re-testing or comparing suspect information to that contained in or re-derived from source material, back-up files, and/or archives). However, unless all responsible inspectors and evaluators monitor all announcements of findings, there remains a potential for misleading results being released to the public.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect, not only operations and public confidence in the agency, but also the agency mission. Damage can generally be corrected within reasonable time and resource constraints, but there is a substantial potential threat to public safety in the interim. In some cases, unauthorized modification or destruction of information can result in loss of human life - a ***high***-impact potential.

Recommended Integrity Impact Level: The default integrity impact level recommended for environmental monitoring and forecasting information is ***moderate***.

D.8.1.3 Availability

The effects of disruption of access to or use of environmental monitoring and forecasting information or information systems can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Except

for cases of emergency bulletins necessary to correct existing threats to public safety, the nature of environmental monitoring and forecasting processes is usually tolerant of reasonable delays. Use of basic procedures and controls, such as alternate communications media and retention of copies of source material, can generally prevent major compromise of mission capability.

Recommended Availability Impact Level: Except where emergency publication of life-threatening product deficiencies are delayed for excessive periods, the default availability impact level recommended for environmental monitoring and forecasting information is normally ***low***.

D.8.2 Environmental Remediation Information Type

Environmental remediation supports the immediate and long-term activities associated with the correcting and offsetting of environmental deficiencies or imbalances, including restoration activities. The following security categorization is recommended for the environmental remediation information type:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

D.8.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of environmental remediation information on the immediate and long-term activities of responsible agencies with respect to correcting and offsetting environmental deficiencies or imbalances. Serious adverse effects are likely to result from 1) exposure of information that is premature and not fully checked for accuracy and that can damage public confidence in an organization targeted for remedial action, 2) unauthorized disclosure of information that is proprietary to an organization with which the agency is interacting, 3) unauthorized and premature disclosure of information concerning proposed remediation in time to assist organizations opposing particular remedial actions, and 4) disclosure of an agency's tactics for enforcing remediation in a manner that has an adverse effect on the enforcement action. The consequences of such unauthorized disclosures may have a serious adverse effect on public confidence in the agency, may have a serious adverse effect on agency operations, and may place the agency at a significant disadvantage.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for environmental remediation information is normally ***moderate***.

D.8.2.2 Integrity

The consequences of unauthorized modification to or destruction of environmental remediation information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is normally needed. The consequences of unauthorized modification or destruction of environmental remediation information can generally be overcome if back-up and archiving procedures are adequate and are implemented. In many cases, competent agency personnel should be able to recognize anomalous information (e.g., by comparing suspect information to that contained in source material, back-up files, and/or archives).

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect, not only operations and public confidence in the agency, but also the agency mission. Damage can generally be corrected within reasonable time and resource constraints, but there is a substantial potential threat to public safety in the interim.

Recommended Integrity Impact Level: The default integrity impact level recommended for environmental remediation information is ***low***.

D.8.2.3 Availability

The effects of disruption of access to or use of environmental remediation information or information systems can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Except for cases of emergency bulletins necessary to correct existing threats to public safety, the nature of environmental remediation processes is usually tolerant of reasonable delays. Use of basic procedures and controls, such as alternate communications media and retention of copies of source material, can generally prevent major compromise of mission capability.

Recommended Availability Impact Level: The default availability impact level recommended for environmental remediation information is normally ***low***.

D.8.3 Pollution Prevention And Control Information Type

Pollution prevention and control includes activities associated with the establishment of environmental standards to control the levels of harmful substances emitted into the soil, water and atmosphere. The following security categorization is recommended for the pollution prevention and control information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.8.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of pollution prevention and control information on the abilities of responsible agencies to establish environmental standards to control the levels of harmful substances emitted into the soil, water and atmosphere. Unauthorized disclosure of pollution prevention and control information can result in inadequately coordinated information being erroneously published as agency standards or policy, misunderstandings that prevent or increase the difficulty of promulgating standards, or discrediting of valid proposed standards or policies by exposure of partial information out of context. The consequences of such unauthorized disclosures may have an adverse effect on public confidence in the agency, may have an adverse effect on agency operations, and may place the agency at an operational disadvantage. Most unauthorized disclosure of pollution prevention and control information is likely to have only a limited adverse effect on the affected agency.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for pollution prevention and control information is normally ***low***.

D.8.3.2 Integrity

The consequences of unauthorized modification to or destruction of pollution prevention and control information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is normally needed. The consequences of unauthorized modification or destruction of pollution prevention and control information can generally be overcome if basic procedures and controls are implemented. In many cases, competent agency personnel should be able to recognize anomalous information (e.g., by comparing suspect information to that contained in source material, back-up files, and/or archives).

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect, not only operations and public confidence in the agency, but also the agency mission. Damage can generally be corrected within reasonable time and resource constraints, but there may be a substantial potential threat to public safety in the interim.

Recommended Integrity Impact Level: The default integrity impact level recommended for pollution prevention and control information is ***low***.

D.8.3.3 Availability

The effects of disruption of access to or use of pollution prevention and control information or information systems can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Except for cases of emergency bulletins necessary to correct existing threats to public safety, the nature of pollution prevention and control processes is usually tolerant of reasonable delays. Use of basic procedures and controls, such as alternate communications media and retention of copies of source material, can generally prevent major compromise of mission capability.

Recommended Availability Impact Level: The default availability impact level associated with pollution prevention and control information is normally ***low***.

D.9 Economic Development

Economic Development includes the activities required to promote commercial/industrial development and to regulate the American financial industry to protect investors. It also includes the management and control of the domestic economy and the money supply, and the protection of intellectual property and innovation. Note: The promotion of U.S. business overseas is captured in the function, "International Affairs and Commerce."

D.9.1 Business and Industry Development Information Type

Business/industry development supports activities related to the creation of economic and business opportunities and stimulus, and the promotion of financial and economic

stability for corporations and citizens involved in different types of business. The recommended baseline categorization of the business and industry development information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.9.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of business and industry development information on the ability of responsible agencies to create economic and business opportunities and stimulus, and promote financial and economic stability for corporations and citizens involved in different types of business. The consequences of unauthorized disclosure of most business and industry development information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: There may be some cases for which ***moderate*** confidentiality impact is associated with unauthorized disclosure of business/industry development. For example, unauthorized disclosure of private information concerning individuals or businesses can result in legal expense, serious effects on public confidence in the agency. This can place the agency at a serious disadvantage and requiring extensive corrective actions. Similarly, unauthorized disclosure of details of current agency business and industry development activities and plans can serve to focus opposition and/or give an unfair advantage to competing interests. Consistent premature disclosure of agency plans can cause significant degradation in mission capability.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for business/industry development information is ***low***.

D.9.1.2 Integrity

The consequences of unauthorized modification to or destruction of business and industry development information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. The consequences of unauthorized modification or destruction of business and industry development information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most business and industry development information is ***low***.

D.9.1.3 Availability

The effects of disruption of access to or use of business and industry development information or information systems can usually be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, and the nature of missions supported by business and industry development information is generally tolerant of delay. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can usually be depended on to prevent significant degradation in mission capability and resultant serious or catastrophic consequences.

Recommended Availability Impact Level: The default availability impact level recommended for business and industry development information is ***low***.

D.9.2 Intellectual Property Protection Information Type

Intellectual property protection involves law enforcement activities involving the enforcement of intellectual property including inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. Note that intellectual property protection is an exception to the often-close relationship between impacts to law enforcement information and information systems and the security of critical infrastructures and key national assets. The following security categorization is recommended for the intellectual property protection information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.9.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of intellectual property protection information on the abilities of responsible agencies to enforce intellectual property including inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. In the case of patent activities considerable sensitivity can be associated with technical details of applications involving inventions having military applications and with records concerning deliberations concerning whether or not patents should be withheld for a period as a result of *national security* considerations. In some cases, the patent application information may be determined to be classified or to contain information concerning weapons or weapons systems. In such cases, the information would be *national security information*, hence, outside the scope of this guideline. However, the consequences of unauthorized disclosure of the vast majority of intellectual property protection information will result in, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for intellectual property protection information is ***low***.

D.9.2.2 Integrity

The consequences of unauthorized modification to or destruction of intellectual property protection information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. In the case of intellectual property protection information, there is a high probability that an integrity compromise will be noticed before its consequences are felt. In any case, the effects of modifications to or deletion of this information are generally limited with respect to agency mission capabilities or assets. Any resulting damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for intellectual property protection information is ***low***.

D.9.2.3 Availability

The effects of disruption of access to or use of intellectual property protection information or information systems can usually be repaired within reasonable time and resource constraints. The time frame required for repair is dependent on mitigating procedures and controls. The nature of intellectual property protection processes is tolerant of reasonable delays. In the case of intellectual property protection records, the disruption of access to records can usually be overcome if basic procedures and controls are implemented.

Recommended Availability Impact Level: The default availability impact level recommended for intellectual property protection information is ***low***.

D.9.3 Financial Sector Oversight Information Type

Financial Sector Oversight involves the regulation of private sector firms and markets (stock exchanges, corporations, etc.) to protect investors from fraud, monopolies, and illegal behavior. This also includes deposit protection. The recommended baseline categorization of the financial sector oversight information type follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

D.9.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of financial sector oversight information on the ability of responsible agencies to regulate private sector firms and markets (stock exchanges, corporations, etc.) to protect investors from fraud, monopolies, and illegal behavior. This also includes deposit protection, creation, regulation, and control the nation's currency and coinage supply and demand. While the consequences of unauthorized disclosure of some financial sector oversight information would have only a limited adverse effect on agency operations, agency assets, or individuals, there are significant exceptions. Unauthorized disclosure of much financial sector oversight information can result in major financial consequences. In some cases, premature disclosure of regulatory information can impact major financial markets and damage national banking and finance infrastructures. For example, unauthorized and premature disclosure of a decision to increase the money supply or of an ongoing

securities fraud investigation can have a dramatic effect on financial markets. Unauthorized and premature disclosure to a single institution (e.g., a major banking institution or brokerage house), could damage faith in regulatory institutions and result in even more market disruption and have a severe or catastrophic adverse effect on public confidence in the agency. Even where the consequences are limited to giving an unfair market advantage to a single financial or commercial institution, unauthorized disclosure can have a serious adverse effect on public confidence in the agency and its staff. One may postulate scenarios in which unauthorized disclosure might have a catastrophic effect on national financial/economic institutions, thus creating a ***high*** confidentiality impact. However, the conditions required to create or facilitate, then exploit such scenarios are generally improbable and/or elaborate.

Recommended Confidentiality Impact Level: The recommended default confidentiality impact level for financial sector oversight information is ***moderate.***

D.9.3.2 Integrity

The consequences of unauthorized modification to or destruction of financial sector oversight information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is normally needed. The consequences of unauthorized modification or destruction of financial sector oversight information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. There may be on-line, automated, or semi-automated activities for which integrity threats can be realized before they are detected. Procedures are in place in most Federal financial sector oversight institutions to mitigate the effects of these consequences. Where unauthorized modification or destruction of financial sector oversight information facilitates or enables a catastrophic confidentiality or availability impact scenario, the integrity impact level may be ***high***.

Recommended Integrity Impact Level: The default integrity impact level recommended for most modification or destruction of financial sector oversight information is ***low***.

D.9.3.3 Availability

The effects of disruption of access to or use of financial sector oversight information or information systems can usually be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, and the nature of missions supported by financial sector oversight information is generally tolerant of delay. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can

usually be depended on to prevent significant degradation in mission capability and resultant serious or catastrophic consequences.

Recommended Availability Impact Level: Except where the period of unavailability is long enough to shake the confidence of financial markets, the default availability impact level recommended for financial sector oversight information is ***low***.

D.9.4 Industry Sector Income Stabilization Information Type

Industry Sector Income Stabilization involves all programs and activities devoted to assisting adversely impacted industrial sectors (farming, commercial transportation, etc.) to ensure the continued availability of their services for the American public and the long-term economic stability of these sectors. The general recommended security categorization for the industry sector income stabilization information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, LOW), (**availability**, LOW)}

D.9.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of industry sector income stabilization information on the ability of responsible agencies to assist adversely impacted industrial sectors (farming, commercial transportation, etc.) to ensure the continued availability of their services for the American public and the long-term economic stability of these sectors. In most cases, unauthorized disclosure of industry sector income stabilization information will have only a limited adverse effect on agency operations, assets, or individuals. However, unauthorized premature disclosure of Federal government plans for industry sector income stabilization actions (e.g., grants or subsidies) as well as of government economic forecasts and commentary preliminary to formulation of plans can result in major financial consequences. In some cases, premature disclosure of industry sector income stabilization information can impact major financial markets and damage national banking and finance infrastructures. Unauthorized and premature disclosure to a single institution (e.g., a major manufacturing institution, a major agribusiness institution, or a commodity brokerage house), could damage confidence in economic stabilization institutions and result in even more market disruption and have a severe or catastrophic adverse effect on public confidence in the government. Even where the consequences are limited to giving an unfair market advantage to a single financial or commercial institution, unauthorized disclosure can have a serious adverse effect on public confidence in an agency and its staff. One may postulate scenarios in which unauthorized disclosure might have a catastrophic effect on national financial/economic institutions, thus creating a ***high*** confidentiality impact. However, the conditions required to create or facilitate, then exploit such scenarios are generally improbable and/or elaborate.

Recommended Confidentiality Impact Level: The recommended default confidentiality impact level for industry sector income stabilization information is ***moderate.***

D.9.4.2 Integrity

Industry sector income stabilization activities are not generally time-critical. The consequences of unauthorized modification of industry sector income stabilization information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In most cases, the adverse effects of unauthorized modification to or destruction of industry sector income stabilization information on agency mission functions and public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for industry sector income stabilization information is ***low***.

D.9.4.3 Availability

The effects of disruption of access to or use of industry sector income stabilization information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Loan assistance processes are generally tolerant of delay. Basic procedures and controls can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of industry sector income stabilization information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for industry sector income stabilization information is ***low***.

D.10 Social Services

Community and Social Services includes all activities aimed at creating, expanding, or improving community and social development, social relationships, and social services in the United States. This includes all activities aimed at locality-specific or nationwide social development and general social services. This Line of Business includes general community development and social services programs, as well as earned and unearned benefit programs that promote these objectives.

D.10.1 Homeownership Promotion Information Type

Homeownership Promotion includes activities devoted to assisting citizens interested in buying homes and educating the public as to the benefits of homeownership. Note: Activities devoted to the provision of housing to low-income members of the public are covered under the Housing Assistance mission. The recommended baseline categorization of the homeownership promotion information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.10.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of homeownership promotion information on the ability of responsible agencies to assist

citizens interested in buying homes and educating the public as to the benefits of homeownership. The consequences of unauthorized disclosure of most homeownership promotion information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals).

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for homeownership promotion information is ***low***.

D.10.1.2 Integrity

The consequences of unauthorized modification to or destruction of homeownership promotion information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Special Factors Affecting Integrity Impact Determination: A more serious threat may be that of modification of access control information or mechanisms in order to gain access to privacy information may have significant adverse effects on operations and/or public confidence in the agency, but the damage to the mission would again usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most homeownership promotion information is ***low***.

D.10.1.3 Availability

The effects of disruption of access to or use of most homeownership promotion information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Integrity Impact Level: The default availability impact level recommended for homeownership promotion information is ***low***.

D.10.2 Community and Regional Development Information Type

The Community and Regional Development mission involves activities designed to assist communities in preventing and eliminating blight and deterioration, assist economically distressed communities, and encourage and foster economic development through improved public facilities and resources. The recommended baseline categorization of the community and regional development information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.10.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of community and regional development information on the ability of responsible agencies to assist communities in preventing and eliminating blight and deterioration, assist economically distressed communities, and encourage and foster economic development through improved public facilities and resources. The consequences of unauthorized disclosure of most community and regional development information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals). Another exception might be unauthorized disclosure of information that gives an individual or corporate entity an unfair competitive advantage in obtaining contracts or other funding for development activities.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for community and regional development information is ***low***.

D.10.2.2 Integrity

The consequences of unauthorized modification to or destruction of community and regional development information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. A more serious threat may be that of modification of access control information or mechanisms in order to gain access to privacy information may have significant adverse effects on operations and/or public confidence in the agency, but the damage to the mission would again usually be limited and can generally be corrected within reasonable time and resource constraints. Another threat is that of unauthorized modification of information in order to perpetrate fraud. This might result in harm to individuals, but fraud on a scale likely to do serious harm to agency operations or missions should be detected by monitoring and audit processes.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most community and regional development information is ***low***.

D.10.2.3 Availability

The effects of disruption of access to or use of most community and regional development information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for community and regional development information is ***low***.

D.10.3 Social Services Information Type

Social Services are designed to provide meaningful opportunities for social and economic growth of the disadvantaged sector of the population in order to develop individuals into productive and self-reliant citizens and promote social equity. Included in this category are social welfare services extended to children and adults with special needs, such as the orphaned, neglected, abandoned, disabled, etc. Such services include family life education and counseling, adoption, guardianship, foster family care, rehabilitation services, etc. Note: This mission does not include services that are primarily for income support (Income Security) or are an integral part of some other mission area (e.g., Health, Workforce Management, etc.). The recommended baseline categorization of the social services information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.10.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of social services information on the ability of responsible agencies to provide meaningful opportunities for social and economic growth of the disadvantaged sector of the population in order to develop individuals into productive and self-reliant citizens and promote social equity. The consequences of unauthorized disclosure of most social services information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences include based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals). Other exceptions include unauthorized disclosure of information that might assist criminals to perpetrate fraud, particularly with respect to income security disbursements.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for social services information is ***low***.

D.10.2.2 Integrity

The consequences of unauthorized modification to or destruction of social services information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. A more serious threat may be that of modification of access control information or mechanisms in order to gain access to privacy information may have significant adverse effects on operations and/or public confidence in the agency, but the damage to the mission would again usually be limited and can generally be corrected within reasonable time and resource constraints. Another threat is that of unauthorized modification of information in order to support fraudulent claims. This might result in harm to individuals, but fraud on a scale likely to do serious harm to agency operations or missions should be detected by monitoring and audit processes.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most social services information is ***low***.

D.10.2.3 Availability

The effects of disruption of access to or use of most social services information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for social services information is ***low***.

D.10.4 Postal Services Information Type

Postal Services provide for the timely and consistent exchange and delivery of mail and packages between businesses, organizations, and residents of the United States or between businesses, organizations, and residents of the United States and the rest of the world. It also includes the nation-wide retail infrastructure required to make Postal Services easily accessible to customers. (Note: The commercial function of mail is more closely aligned with the "Business and Industry Development" mission in the "Economic Development mission area." The international commercial function of mail is more closely aligned with the "Global Trade" mission in the "International Affairs" mission area). The recommended baseline categorization of thee postal services information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.10.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of postal services information on the ability of responsible agencies to provide for the timely and consistent exchange and delivery of mail and packages between businesses, organizations, and residents of the United States or between businesses, organizations, and residents of the United States and the rest of the world. The consequences of unauthorized disclosure of

most postal services information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences include based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals). Other exceptions include unauthorized disclosure of information that might assist criminals to perpetrate fraud, particularly with respect to income security disbursements. Where unauthorized disclosure of access control information might assist terrorists to gain access to postal facilities for purposes of implementing an attack, the confidentiality impact can be ***high***. Also, since registered mail can be employed to transmit classified information, information regarding some registered mail can conceivably facilitate unauthorized access to *national security* information.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most postal services information is ***low***.

D.10.2.2 Integrity

The consequences of unauthorized modification to or destruction of postal services information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Special Factors Affecting Integrity Impact Determination: A more serious threat may be that of modification of access control information or mechanisms in order to gain access to privacy information may have significant adverse effects on operations and/or public confidence in the agency, but the damage to the mission would again usually be limited and can generally be corrected within reasonable time and resource constraints. Where the compromise of access control mechanisms might assist terrorists to use postal facilities to carry out an attack, the consequences in terms of critical infrastructure protection and risk to human life can be severe. In such cases, the integrity impact of compromise would be ***high***. Another threat is that of unauthorized modification of information in order to support fraudulent activities (e.g., misdirection of monetary instruments, execution of fraudulent financial transactions). This might result in harm to individuals, but fraud on a scale likely to do serious harm to agency operations or missions should be detected by monitoring and audit processes.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most postal services information is ***moderate***.

D.10.2.3 Availability

The effects of disruption of access to or use of most postal services information or information systems would have, an adverse effect on agency operations, the severity of which would depend on the extent and duration of the outage. Extended widespread outages could seriously affect the commerce of the United States.

Recommended Availability Impact Level: The default availability impact level recommended for postal services information is ***moderate***.

D.11 Transportation

Transportation involves all federally supported activities related to the safe passage, conveyance, or transportation of goods and/or people. Note that impacts to some information and many information systems associated with transportation activities may affect the security of, not only the transportation infrastructure, but also to a broad range of other critical infrastructures and key national assets.

D.11.1 Ground Transportation Information Type

Ground Transportation involves the activities related to ensuring the availability of transit and the safe passage of passengers and goods over land. Note: The protection of ground transportation from deliberate attack is included in the Transportation Security information type under the Homeland Security mission area. The general recommended security categorization for the ground transportation information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.11.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of ground transportation information on the ability of responsible agencies to ensure the availability of transit and the safe passage of passengers and goods over land. As indicated above, the protection of ground transportation from deliberate attack is included in the Transportation Security information type under the Homeland Security mission area. Some regulatory and tariff enforcement functions associated with the safe passage of passengers and goods over land involve relatively sensitive information. These are treated under Law Enforcement (see D.16). Also, unauthorized disclosure of accident investigation information that has not yet been adequately researched, coordinated, or edited can result in serious economic harm to individuals and to corporations. Loss in public confidence is a further potential consequence. Additionally, some information associated with ground transportation functions is proprietary to corporations or subject to privacy laws (e.g., the Privacy Act of 1974, HIPAA). In such cases, the confidentiality impact resulting from unauthorized disclosure can be ***moderate***. Note that some military ground transportation information is *national security information* and is outside the scope of this guideline. However, most cases, unauthorized disclosure of ground transportation information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for ground transportation information is ***low***.

D.11.1.2 Integrity

Some ground transportation functions are time-critical (e.g., track switching functions associated with rail travel). Unauthorized modification to or destruction of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Such information would have a ***high*** integrity impact level. However, the consequences of unauthorized modification of most ground transportation information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In most cases, the adverse effects of unauthorized modification to or destruction of ground transportation information on agency mission functions and public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for ground transportation information is ***low***.

D.11.1.3 Availability

Some ground transportation functions are time-critical (e.g., track switching functions associated with rail travel). Loss of availability of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Such information would have a ***high*** integrity impact level. However, the effects of disruption of access to or use of most ground transportation information can usually be repaired. The time frame required for repair is dependent on implementation and use of adequate back up information, facilities and procedures. Most ground transportation processes are tolerant of reasonable delays. Availability and use of basic mitigating procedures and controls can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of ground transportation information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for ground transportation information is ***low***.

D.11.2 Water Transportation Information Type

Water Transportation involves the activities related to ensuring the availability of transit and the safe passage of passengers and goods over sea and water. Note: The protection of maritime transportation from deliberate attack is included in the Transportation Security information type under the Homeland Security mission area. The general recommended security categorization for the water transportation information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.11.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of water transportation information on the ability of responsible agencies to ensure the availability of transit and the safe passage of passengers and goods over sea and water. As indicated above, the protection of water transportation from deliberate attack is included in the Transportation Security information type under the Homeland Security mission area. Some regulatory and tariff enforcement functions associated with the safe passage of passengers and goods over sea and water involve relatively sensitive information. These are treated under Law Enforcement (see C16). Also, unauthorized disclosure of accident investigation information that has not yet been adequately researched, coordinated, or edited can result in serious economic harm to individuals and to corporations. Loss in public confidence is a further potential consequence. Additionally, some information associated with water transportation functions is proprietary to corporations or subject to privacy laws. In such cases, the confidentiality impact resulting from unauthorized disclosure can be ***moderate***. Note that some military sea and water transportation information is *national security information* and is outside the scope of this guideline. However, most cases, unauthorized disclosure of water transportation information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for water transportation information is ***low***.

D.11.2.2 Integrity

Some water and sea transportation functions are time-critical (e.g., distress signals, docking operations, collision avoidance, warnings of hazardous weather or sea conditions). Unauthorized modification to or destruction of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Such information would have a ***high*** integrity impact level. However, the consequences of unauthorized modification of most water transportation information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In most cases, the adverse effects of unauthorized modification to or destruction of water transportation information on agency mission functions and public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for water transportation information is ***low***.

D.11.2.3 Availability

Some water and sea transportation functions are time-critical (e.g., distress signals, docking operations, collision avoidance, warnings of hazardous weather or sea conditions). Loss of availability of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Such information would have a ***high*** integrity impact level. However, the effects of disruption of access to or use of most water transportation information can usually be

repaired. The time frame required for repair is dependent on mitigating procedures and controls. Most water transportation processes are tolerant of reasonable delays. Basic procedures and controls can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of water transportation information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for water transportation information is ***low***.

D.11.3 Air Transportation Information Type

Air Transportation involves the activities related to the safe passage of passengers or goods through the air. It also includes command and control activities related to the safe movement of aircraft through all phases of flight for commercial and military operations. Note: The protection of air transportation from deliberate attack is included in the Transportation Security information type under the Homeland Security mission area. The general recommended security categorization for the air transportation information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, HIGH), (**availability**, HIGH)}

D.11.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of air transportation information on the ability of responsible agencies to ensure the availability of transit and the safe passage of passengers and goods through the air. As indicated above, the protection of air transportation from deliberate attack is included in the Transportation Security information type under the Homeland Security mission area. Some regulatory and tariff enforcement functions associated with the safe passage of passengers and goods over land involve relatively sensitive information. These are treated under Law Enforcement (see D.16). Also, unauthorized disclosure of accident investigation information that has not yet been adequately researched, coordinated, or edited can result in serious economic harm to individuals and to corporations. Loss in public confidence is a further potential consequence. Additionally, some information associated with air transportation functions is proprietary to corporations or subject to privacy laws. In such cases, the confidentiality impact resulting from unauthorized disclosure can be ***moderate***. The sensitivity of air transportation information can be time or event-driven. For example, passenger lists are not releasable to the general public before a flight takes off, but are placed in the public domain in the event of a crash. Also, much military air transport information is *national security information*. As such, it is outside the scope of this guideline. However, most cases, unauthorized disclosure of air transportation information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for air transportation information is ***low***.

D.11.3.2 Integrity

Air transportation is characterized by high speeds, high traffic loads, and time stress. Many air transportation functions are time-critical (e.g., air traffic control instructions, position reports, weather reports for the terminal area, maintenance trouble reports). Unauthorized modification to or destruction of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Such information would have a ***high*** integrity impact level. While the consequences of unauthorized modification of some air transportation information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented, the short time often available between occurrence of anomalies and realization of catastrophic consequences suggest a relatively high integrity impact level. Where it is reasonable to assume that agency personnel will be able to recognize anomalous information and compare suspect information to that contained in source materials before the effects of modification or loss of information is felt, a lower integrity impact level applies.

Recommended Integrity Impact Level: For flight operations, the default integrity impact level recommended for air transportation information is ***high***.

D.11.3.3 Availability

Air transportation is characterized by high speeds, high traffic loads, and time stress. Many air transportation functions are time-critical (e.g., air traffic control instructions, position reports, weather reports for the terminal area, maintenance trouble reports). Loss of availability of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Such information would have a ***high*** integrity impact level. Timing plays a large part in the availability impact of air transportation information. For example, the time criticality of weather information may be measured in minutes or hours in the case of pre-flight and mid-flight operations. However, on final landing approach, up to the second availability can be required (e.g., detection of microbursts in the terminal area). While the effects of disruption of access to or use of some air transportation information can usually be repaired, air operations are not all tolerant of information loss. The time frame required for information systems recovery is dependent on mitigating procedures and controls.

Special Factors Affecting Availability Impact Determination: Many air transportation processes rely on systems redundancy to prevent catastrophic loss of availability of critical information. Basic mitigating procedures and controls can usually prevent serious or catastrophic damage to mission capability. Where such procedures controls are in place, the availability impact level assigned to individual information systems may be ***low***.

Recommended Availability Impact Level: At the air traffic control system level (system of systems), the recommended default availability impact level for air transportation information is ***high***.

D.11.4 Space Operations Information Type

Space Operations involves the activities related to the safe launches/missions of passengers or goods into aerospace and includes commercial, scientific, and military operations. The recommended security categorization for the space operations information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, HIGH), (**availability**, HIGH)}

D.11.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of space operations information on the ability of responsible agencies to conduct safe launches/missions of passengers or goods into aerospace and includes commercial, scientific, and military operations. The protection of space operations from deliberate attack involves military operations (D.1), homeland security operations (D.2), and law enforcement operations (D.16). Some information regarding space operations (particularly military operations) is classified *national security information* and is outside the scope of this guideline. Civilian space operations are supposed to be conducted in the open. Administrative and business functions associated with space operations may involve proprietary, procurement-sensitive, and Privacy Act information. In such cases, the confidentiality impact resulting from unauthorized disclosure can be ***moderate***. However, in most cases, unauthorized disclosure of space operations information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for space operations information is ***low***.

D.11.4.2 Integrity

Space operations are characterized by high speeds, critical operational timing and safety parameters, and low tolerance for error. Unauthorized modification to or destruction of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Such information would have a ***high*** integrity impact level. While the consequences of unauthorized modification of some space operations information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are used, the short time often available between occurrence of anomalies and realization of catastrophic consequences suggest a relatively high integrity impact level.

Special Factors Affecting Integrity Impact Determination: Where it is reasonable to assume that agency personnel will be able to recognize anomalous information and compare suspect information to that contained in source materials before the effects of modification or loss of information is felt, a lower integrity impact level may apply.

Recommended Integrity Impact Level: For flight operations, the default integrity impact level recommended for space operations information is ***high***.

D.11.4.3 Availability

Space operations are characterized by high speeds, critical operational timing and safety parameters, and low tolerance for error. Loss of availability of time-critical information necessary to these functions can result in large-scale property loss and in loss of human lives. Such information would have a ***high*** integrity impact level. Timing plays a large part in the availability impact of space operations information. While the effects of disruption of access to or use of some space operations information can usually be repaired, air operations are not all tolerant of information loss.

Special Factors Affecting Availability Impact Determination: The time frame required for information systems recovery is dependent on mitigating procedures and controls. Many space operations processes rely on systems redundancy to prevent catastrophic loss of availability of critical information. However, every effort is made to ensure the correct functionality of each of the components. Availability and use of basic procedures and controls (e.g., back-up files, alternate facilities, and contingency procedures) can often prevent serious or catastrophic damage to mission capability.

Recommended Availability Impact Level: The recommended default availability impact level for space operations information is ***high***.

D.12 Education

Education refers to those activities that impart knowledge or understanding of a particular subject to the public. Education can take place at a formal school, college, university or other training program. This mission area includes all government programs that promote the education of the public, including both earned and unearned benefit programs.

D.12.1 Elementary, Secondary, and Vocational Education Information Type

Elementary, secondary, and vocational education refers to the provision of education in elementary subjects (reading and writing and arithmetic); education provided by a high school or college preparatory school; and vocational and technical education and training. The recommended baseline categorization of the elementary, secondary, and vocational education information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.12.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of elementary, secondary, and vocational education information on the ability of responsible agencies to provide guidance and consultative services. The consequences of unauthorized disclosure of most elementary, secondary, and vocational education information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for elementary, secondary, and vocational education information is ***low***.

D.12.1.2 Integrity

The consequences of unauthorized modification to or destruction of elementary, secondary, and vocational education information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most elementary, secondary, and vocational education information is ***low***.

D.12.1.3 Availability

The effects of disruption of access to or use of most elementary, secondary, and vocational education information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for elementary, secondary, and vocational education information is ***low***.

D.12.2 Higher Education Information Type

Higher Education refers to education beyond the secondary level; specifically, education provided by a college or university. It includes external higher educational activities performed by the government (e.g., Military Academies, ROTC, and USDA Graduate School). The recommended baseline categorization of the higher education information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.12.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of higher education information on the ability of responsible agencies to support education beyond the secondary level (e.g., Military Academies, ROTC, USDA Graduate School, and other public and private universities and colleges). The consequences of unauthorized disclosure of most higher education information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Exceptions that might have a potential for more serious consequences are based on the mission supported by the external training and education activity. In such cases, the impact on the system is defined by that established by information associated with the supported mission.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for higher education information is ***low***.

D.12.2.2 Integrity

The consequences of unauthorized modification to or destruction of higher education information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Exceptions that might have a potential for more serious consequences are based on the mission supported by the higher education activity (e.g., undetected modification of weapons training information at a service academy where the modification could result in harm to the student or other individuals). In such cases, the impact on the system is defined by that established by information associated with the supported mission.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most higher education information is ***low***.

D.12.2.3 Availability

The effects of disruption of access to or use of most higher education information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for higher education information is ***low***.

D.12.3 Cultural and Historic Preservation Information Type

Cultural and Historic Preservation involves all activities performed by the Federal Government to collect and preserve information and artifacts important to the culture and history of the United States and its citizenry and the education of U.S. citizens and the world. The recommended baseline categorization of the cultural and historic preservation information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.12.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of cultural and historic preservation information on the ability of responsible agencies to collect and preserve information and artifacts important to the culture and history of the United States and its citizenry and the education of U.S. citizens and the world. The consequences of unauthorized disclosure of most cultural and historic preservation information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In cases where disclosure of information might be useful to an individual or organization intent on destruction of historical materials, the potential consequences to key national assets could be serious to severe. In such cases, the confidentiality impact could be ***moderate*** to ***high***.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for cultural and historic preservation information is ***low***.

D.12.3.2 Integrity

The consequences of unauthorized modification to or destruction of cultural and historic preservation information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Special Factors Affecting Integrity Impact Determination: In cases where undetected modification of information might be useful to an individual or organization intent on destruction of historical materials, the potential consequences to key national assets could be serious to severe. In such cases, the integrity impact could be ***moderate*** to ***high***.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most cultural and historic preservation information is ***low***.

D.12.3.3 Availability

The effects of disruption of access to or use of most cultural and historic preservation information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for cultural and historic preservation information is ***low***.

D.12.4 Cultural and Historic Exhibition Information Type

Cultural and Historic Exhibition includes all activities undertaken by the U.S. government to promote education through the exhibition of cultural, historical, and other information, archives, art, etc. The recommended baseline categorization of the cultural and historic exhibition information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.12.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of cultural and historic exhibition information on the ability of responsible agencies to promote education through the exhibition of cultural, historical, and other information, archives,

art, etc. The consequences of unauthorized disclosure of most cultural and historic exhibition information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: In cases where disclosure of information might be useful to an individual or organization intent on destruction of historical materials or archives, the potential consequences to key national assets could be serious to severe. In such cases, the confidentiality impact could be ***moderate*** to ***high***.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for cultural and historic exhibition information is ***low***.

D.12.4.2 Integrity

The consequences of unauthorized modification to or destruction of cultural and historic exhibition information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. In cases where undetected modification of information might be useful to an individual or organization intent on destruction of historical materials or archives, the potential consequences to key national assets could be serious to severe. In such cases, the integrity impact could be ***moderate*** to ***high***.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most cultural and historic exhibition information is ***low***.

D.12.4.3 Availability

The effects of disruption of access to or use of most cultural and historic exhibition information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for cultural and historic exhibition information is ***low***.

D.13 Workforce Management

Workforce Management includes those activities that promote the welfare of the Nation's workforce by improving their working conditions, advancing opportunities for profitable employment, and strengthening free collective bargaining.

D.13.1 Training and Employment Information Type

Training and Employment includes programs of job or skill training, employment services and placement, and programs to promote the hiring of marginal, unemployed, or

low-income workers. The recommended baseline categorization of the training and employment information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.13.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of training and employment information on the ability of responsible agencies to provide job or skill training, employment services and placement, and programs to promote the hiring of marginal, unemployed, or low-income workers. The consequences of unauthorized disclosure of most training and employment information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals).

Special Factors Affecting Confidentiality Impact Determination: The default confidentiality impact recommended for training and employment information is ***low***.

D.13.1.2 Integrity

The consequences of unauthorized modification to or destruction of training and employment information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. Modification of access control information or mechanisms in order to gain access to privacy information may have significant adverse effects on operations and/or public confidence in the agency, but the damage to the mission would again usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most training and employment information is ***low***.

D.13.1.3 Availability

The effects of disruption of access to or use of most training and employment information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for training and employment information is ***low***.

D.13.2 Labor Rights Management Information Type

Labor Rights Management refers to those activities undertaken to ensure that employees and employers are aware of and comply with all statutes and regulations concerning labor rights, including those pertaining to wages, benefits, safety and health, whistleblower, and nondiscrimination policies. The recommended baseline categorization of the labor rights management information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.13.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of labor rights management information on the ability of responsible agencies to ensure that employees and employers are aware of and comply with all statutes and regulations concerning labor rights, including those pertaining to wages, benefits, safety and health, whistleblower, and nondiscrimination policies. In some cases, premature release of draft labor rights bulletins might adversely affect the effectiveness of agency operations. In general, though, the consequences of unauthorized disclosure of most labor rights management information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for labor rights management information is ***low***.

D.13.2.2 Integrity

The consequences of unauthorized modification to or destruction of labor rights management information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most labor rights management information is ***low***.

D.13.2.3 Availability

The effects of disruption of access to or use of most labor rights management information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for labor rights management information is ***low***.

D.13.3 Worker Safety Information Type

Worker Safety refers to those activities undertaken to save lives, prevent injuries, and protect the health of America's workers. The recommended baseline categorization of the worker safety information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.13.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of worker safety information on the ability of responsible agencies to protect the health and safety of America's workers. In some cases, premature release of draft worker safety bulletins might adversely affect the effectiveness of agency operations. In general, though, the consequences of unauthorized disclosure of most worker safety information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for worker safety information is ***low***.

D.13.3.2 Integrity

The consequences of unauthorized modification to or destruction of worker safety information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most worker safety information is ***low***.

D.13.3.3 Availability

The effects of disruption of access to or use of most worker safety information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for worker safety information is ***low***.

D.14 Health

Health involves Federal programs and activities charged with ensuring and providing for the health and well being of the public. This includes the direct provision of health care services and immunizations as well as the monitoring and tracking of public health indicators for the detection of trends and identification of widespread illnesses/diseases. It also includes both earned and unearned health care benefit programs. Note that impacts

to some public health information and information systems may affect the security of critical elements of the public health infrastructure.

D.14.1 Illness Prevention Information Type

Illness prevention supports activities associated with the prevention and mitigation of illness and diseases. Note that impacts to some information and information systems associated with illness prevention (e.g., the Centers for Disease Control) may affect the security the public health infrastructure. In such cases, integrity and availability impacts can be ***high***. However, in general, the following security categorization is recommended for the illness prevention information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.14.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of illness prevention information on the ability of responsible agencies to prevent and mitigate illness and diseases. Most consequences of unauthorized disclosure of illness prevention information are unlikely to have a serious adverse effect on agency operations.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for illness prevention information is normally ***low***.

D.14.1.2 Integrity

The consequences of unauthorized modification or destruction of illness prevention information can be serious if its nature and timing results in exposure of the public to incorrect medical advice, mislabeled, tainted, or otherwise harmful drugs. In many cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives. However, unless all responsible personnel monitor all announcements of findings, there remains a potential for misleading information to be released to the public.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications that contain illness prevention information (e.g., web pages, electronic mail) may adversely affect, not only operations and public confidence in the agency, but also the agency mission. Damage can generally be corrected within reasonable time and resource constraints, but there is a substantial potential threat to public safety in the interim. In some cases, undetected and unauthorized modification or destruction of illness prevention information can result in loss of human life.

Recommended Integrity Impact Level: The default integrity impact level recommended for illness prevention information is ***low***.

D.14.1.3 Availability

The effects of disruption of access to or use of illness prevention information or information systems can usually be repaired. The time frame required for repair is

dependent on mitigating procedures and controls. Except for cases of emergency bulletins necessary to correct urgent threats to public health, the nature of illness prevention processes is usually tolerant of reasonable delays. Basic procedures and controls (e.g., use of alternate communications media and retention of copies of source material) can generally prevent major compromise of mission capability.

Special Factors Affecting Availability Impact Determination: Where emergency communications necessary to deal with life-threatening situations are delayed for excessive periods, the availability impact level can be ***high***.

Recommended Availability Impact Level: The default integrity level recommended for illness prevention information is ***low***.

D.14.2 Immunization Management Information Type

Immunization management includes all activities associated with the preparation, storage, and use of inoculations and vaccinations. The following security categorization is recommended for the immunization management information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.14.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of immunization management information on the ability of responsible agencies to prepare, store, and use inoculations and vaccinations. Most consequences of unauthorized disclosure of immunization management information are unlikely to have a serious adverse effect on agency operations.

Special Factors Affecting Confidentiality Impact Determination: Some information associated with immunization management involves confidential patient information subject to the Privacy Act and to HIPPA. Other information (e.g., information proprietary to vaccine developers and vendors) must be protected under rules governing proprietary information and procurement management.

Recommended Confidentiality Impact Level: In general, the default confidentiality impact level recommended for most immunization management information is ***low***.

D.14.2.2 Integrity

The consequences of unauthorized modification or destruction of immunization management information can be serious if its nature and timing results in exposure of the public to incorrect or tainted medication or dosages. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: There remains some potential for incorrect information regarding age, storage history, or recommended dosage of vaccines. Unauthorized modification or destruction of information affecting external

communications that contain immunization management information (e.g., web pages, electronic mail) may adversely affect, not only operations and public confidence in the agency, but also the agency mission. Damage can generally be corrected within reasonable time and resource constraints, but there is a substantial potential threat to public safety in the interim. In some cases, undetected and unauthorized modification or destruction of immunization management information can result in loss of human life.

Recommended Integrity Impact Level: The default integrity impact level recommended for immunization management information is ***low***.

D.14.2.3 Availability

The effects of disruption of access to or use of immunization management information or information systems can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Except for cases of emergency bulletins necessary to correct urgent threats to public health, the nature of immunization management processes is usually tolerant of reasonable delays. Use of Basic procedures and controls, such as alternate communications media and retention of copies of source material, can generally prevent major compromise of mission capability.

Special Factors Affecting Availability Impact Determination: There may be activities in which there is potential for emergency communications necessary to deal with life-threatening situations are delayed for excessive periods.

Recommended Availability Impact Level: The default availability impact level recommended for immunization management information is ***low***.

D.14.3 Public Health Monitoring Information Type

Public health monitoring involves activities associated with monitoring the public health and tracking the spread of disease. The following security categorization is recommended for the public health monitoring information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.14.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of public health monitoring information on the ability of responsible agencies to monitor public health and track the spread of disease. Most consequences of unauthorized disclosure of public health monitoring information are unlikely to have a serious adverse effect on agency operations.

Special Factors Affecting Confidentiality Impact Determination: Much information associated with public health monitoring involves confidential patient information subject to the Privacy Act and to HIPPA.

Recommended Confidentiality Impact Level: The confidentiality impact level recommended for most public health monitoring information is ***low***.

D.14.3.2 Integrity

The consequences of unauthorized modification or destruction of public health monitoring information can be serious if the modification or destruction is not detected before it is acted upon. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: There remains some potential for incorrect information resulting in delayed reaction to serious health threats and/or inappropriate allocation/deployment of health care services. Unauthorized modification or destruction of information affecting external communications that contain public health monitoring information (e.g., web pages, electronic mail) may adversely affect, not only operations and public confidence in the agency, but also the agency mission. Damage can generally be corrected within reasonable time and resource constraints, but there is a substantial potential threat to public safety in the interim. In some cases, undetected and unauthorized modification or destruction of public health monitoring information can result in loss of human life.

Recommended Integrity Impact Level: The default integrity impact level recommended for public health monitoring information is ***low***.

D.14.3.3 Availability

The effects of disruption of access to or use of public health monitoring information or information systems can usually be repaired. The time frame available is dependent on the severity of the health threat(s) and the rapidity with which the threat is spreading/growing. The time frame required for repair is dependent on mitigating procedures and controls. Except for cases of monitoring information necessary to generate emergency bulletins necessary to correct urgent threats to public health, the nature of public health monitoring processes is usually tolerant of reasonable delays. Use of Basic procedures and controls, such as alternate communications media and retention of copies of source material, can generally prevent major compromise of mission capability.

Special Factors Affecting Availability Impact Determination: There are circumstances under which there is a potential for emergency processing necessary to deal with life-threatening situations to be delayed for excessive periods.

Recommended Availability Impact Level: The default availability impact level recommended for public health monitoring information is ***low***.

D.14.4 Health Care Services Information Type

Health Care Services involves programs and activities that directly provide health and medical care to the American public, including both earned and unearned health care benefit programs. The following security categorization is recommended for the health care information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.14.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of health services care information on the ability of responsible agencies to directly provide health and medical care to the American public, including both earned and unearned health care benefit programs. Most consequences of unauthorized disclosure of health care information are unlikely to have a serious adverse effect on agency operations.

Special Factors Affecting Confidentiality Impact Determination: Some information associated with health care involves confidential patient information subject to the Privacy Act and to HIPPA. Other information (e.g., information proprietary to hospitals, pharmaceutical companies, insurers, and care givers) must be protected under rules governing proprietary information and procurement management.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most health care information is ***low***.

D.14.4.2 Integrity

Many activities associated with health care services are not generally time critical. The consequences of unauthorized modification of non-time critical information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In most cases, the adverse effects of unauthorized modification to or destruction of non-time critical information on agency mission functions and/or public confidence in the agency can be expected to be limited.

Special Factors Affecting Integrity Impact Determination: The consequences of unauthorized modification or destruction of health care information can be serious if its nature and timing results in incorrect, inappropriate, or excessively delayed treatment of patients. In these cases, serious adverse effects can include expensive and disruptive legal actions and danger to human life. Unauthorized modification or destruction of information affecting external communications that contain health care information (e.g., web pages, electronic mail) may adversely affect, not only operations and public confidence in the agency, but also the agency mission. Damage can generally be corrected within reasonable time and resource constraints, but there is a substantial potential threat to public safety in the interim.

Recommended Integrity Impact Level: Because of the potential for undetected and unauthorized modification or destruction of health care information to result in loss of human life, the default integrity impact level recommended for health care information is ***high***.

D.14.4.3 Availability

The effects of disruption of access to or use of health care information or information systems can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Except for cases of emergency actions necessary to correct urgent threats to patient health, the nature of health care processes is usually tolerant of reasonable delays. Use of basic procedures and controls, such as alternate communications media and retention of copies of source material, can generally prevent major compromise of mission capability.

Special Factors Affecting Availability Impact Determination: There may be circumstances under which emergency communications necessary to deal with life-threatening situations are delayed for excessive periods.

Recommended Availability Impact Level: The default availability impact level recommended for health care information is ***low***.

D.14.5 Consumer Health and Safety Information Type

Consumer Health and Safety supports activities associated with the inspection, education, and evaluation of consumer products to assess the potential risks and dangers they may present to the consumer (both humans and animals), (i.e. food, cosmetics, pharmaceuticals, and other consumer products). Note that impacts to some information and information systems associated with quality assurance of food and pharmaceuticals may affect the security of critical agriculture and food and public health infrastructures. In such cases, integrity and availability impacts can be ***high***. However, in general, the following security categorization is recommended for the consumer health and safety information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

D.14.5.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of consumer health and safety information on the ability of responsible agencies to perform inspection, education and evaluation functions involving food, pharmaceuticals and other consumer products. Most consequences of unauthorized disclosure of consumer health and safety information are unlikely to have a serious adverse effect on agency operations. Due diligence with respect to legal procedures can generally mitigate consequences.

Special Factors Affecting Confidentiality Impact Determination: The most serious adverse effects are likely to involve exposure of information that is proprietary to an organization being evaluated by the agency. [Note that unauthorized disclosure of some information can have serious economic impact on both individual companies and the broader market place (e.g., short-term stock market perturbations). The consequences of such unauthorized disclosures may have an adverse effect on public confidence in the agency, and may include short-term staffing challenges for the agency.]

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for consumer health and safety information is ***low***.

D.14.5.2 Integrity

The consequences of unauthorized modification or destruction of consumer health and safety information can be serious if its nature and timing results in exposure of the public to mislabeled, tainted, or otherwise harmful food, drugs, or consumer products. In many cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives. However, unless all responsible inspectors and evaluators monitor all announcements of findings, there remains a potential for misleading results to be released to the public.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect, not only operations and public confidence in the agency, but also the agency mission. Damage can generally be corrected within reasonable time and resource constraints, but there is a substantial potential threat to public safety in the interim. In some cases, unauthorized modification or destruction of information can result in loss of human life.

Recommended Integrity Impact Level: Even given the implementation of basic procedures and controls (e.g., monitoring and alternate communications procedures for inspection and evaluation activities involving life-threatening consequences), the default integrity impact level recommended for consumer health and safety information remains at least ***moderate***.

D.14.5.3 Availability

The effects of disruption of access to or use of consumer health and safety information or information systems can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Except for cases of emergency bulletins necessary to correct existing threats to public safety, the nature of consumer products quality assurance processes is usually tolerant of reasonable delays. Use of basic procedures and controls, such as alternate communications media and retention of copies of source material, can generally prevent major compromise of mission capability.

Special Factors Affecting Availability Impact Determination: There may be circumstances under which emergency communication of information regarding life-threatening product deficiencies is delayed for excessive periods.

Recommended Availability Impact Level: The default availability impact level recommended for consumer health and safety information is ***low***.

D.15 Income Security

Income Security includes activities designed to ensure that members of the public are provided with the necessary means – both financial and otherwise – to sustain an

adequate level of existence. This includes all benefit programs, both earned and unearned, that promote these goals for members of the public.

D.15.1 General Retirement and Disability Information Type

General Retirement and Disability involves the development and management of retirement benefits, pensions, and income security for those who are retired or disabled. The recommended baseline categorization of the general retirement and disability information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.15.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of general retirement and disability information on the ability of responsible agencies to develop and manage of retirement benefits, pensions, and income security for those who are retired or disabled. The consequences of unauthorized disclosure of most general retirement and disability information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals).

Recommended Confidentiality Impact Level: The confidentiality impact recommended for general retirement and disability information is ***low***.

D.15.1.2 Integrity

The consequences of unauthorized modification to or destruction of general retirement and disability information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Special Factors Affecting Integrity Impact Determination: A more serious threat may be that of modification of access control information or mechanisms in order to gain access to privacy information may have significant adverse effects on operations and/or public confidence in the agency, but the damage to the mission would again usually be limited and can generally be corrected within reasonable time and resource constraints. Another threat is that of unauthorized modification of information in order to perpetrate fraud (e.g., creation of false accounts or diversion of payments). This might result in harm to individuals, but fraud on a scale likely to do serious harm to agency operations or missions should be detected by monitoring and audit processes.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most general retirement and disability information is ***low***.

D.15.1.3 Availability

The effects of disruption of access to or use of most general retirement and disability information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for general retirement and disability information is ***low***.

D.15.2 Unemployment Compensation Information Type

Unemployment Compensation provides income security to those who are no longer employed, while they seek new employment. The recommended baseline categorization of the unemployment compensation information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.15.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of unemployment compensation information on the ability of responsible agencies to provide income security to those who are no longer employed, while they seek new employment. The consequences of unauthorized disclosure of most unemployment compensation information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals).

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for unemployment compensation information is ***low***.

D.15.2.2 Integrity

The consequences of unauthorized modification to or destruction of unemployment compensation information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Special Factors Affecting Integrity Impact Determination: A more serious threat may be that of modification of access control information or mechanisms in order to gain access to privacy information may have significant adverse effects on operations and/or public confidence in the agency, but the damage to the mission would again usually be limited and can generally be corrected within reasonable time and resource constraints. Another threat is that of unauthorized modification of information in order to perpetrate fraud (e.g., creation of false accounts or diversion of payments). This might result in harm to individuals, but fraud on a scale likely to do serious harm to agency operations or missions should be detected by monitoring and audit processes.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most unemployment compensation information is ***low***.

D.15.2.3 Availability

The effects of disruption of access to or use of most unemployment compensation information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for unemployment compensation information is ***low***.

D.15.3 Housing Assistance Information Type

Housing Assistance involves the development and management programs that provide housing to those who are unable to provide housing for themselves including the rental of single-family or multifamily properties, and the management and operation of federally supported housing properties. The recommended baseline categorization of the housing assistance information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.15.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of housing assistance information on the ability of responsible agencies to develop and manage programs that provide housing to those who are unable to provide housing for themselves including the rental of single-family or multifamily properties, and the management and operation of federally supported housing properties. The consequences of unauthorized disclosure of most housing assistance information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals).

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for housing assistance information is ***low***.

D.15.3.2 Integrity

The consequences of unauthorized modification to or destruction of housing assistance information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Special Factors Affecting Integrity Impact Determination: A more serious threat may be that of modification of access control information or mechanisms in order to gain access to privacy information may have significant adverse effects on operations and/or public confidence in the agency, but the damage to the mission would again usually be limited and can generally be corrected within reasonable time and resource constraints. Another threat is that of unauthorized modification of information in order to perpetrate fraud. This might result in harm to individuals, but fraud on a scale likely to do serious harm to agency operations or missions should be detected by monitoring and audit processes.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most housing assistance information is ***low***.

D.15.3.3 Availability

The effects of disruption of access to or use of most housing assistance information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for housing assistance information is ***low***.

D.15.4 Food and Nutrition Assistance Information Type

Food and Nutrition Assistance involves the development and management of programs that provide food and nutrition assistance to those members of the public who are unable to provide for these needs themselves. The recommended baseline categorization of the food and nutrition assistance information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.15.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of food and nutrition assistance information on the ability of responsible agencies to develop and manage of programs that provide food and nutrition assistance to those members of the public who are unable to provide for these needs themselves. The consequences of

unauthorized disclosure of most food and nutrition assistance information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals).

Recommended Confidentiality Impact Level: The confidentiality impact recommended for food and nutrition assistance information is ***low***.

D.15.4.2 Integrity

The consequences of unauthorized modification to or destruction of food and nutrition assistance information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. A more serious threat may be that of modification of access control information or mechanisms in order to gain access to privacy information may have significant adverse effects on operations and/or public confidence in the agency, but the damage to the mission would again usually be limited and can generally be corrected within reasonable time and resource constraints. Another threat is that of unauthorized modification of information in order to perpetrate fraud. This might result in harm to individuals, but fraud on a scale likely to do serious harm to agency operations or missions should be detected by monitoring and audit processes.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most food and nutrition assistance information is ***low***.

D.15.4.3 Availability

The effects of disruption of access to or use of most food and nutrition assistance information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for food and nutrition assistance information is ***low***.

D.15.5 Survivor Compensation Information Type

Survivor Compensation provides compensation to the survivors of individuals currently receiving or eligible to receive benefits from the Federal Government. This includes, but is not limited to, survivors such as spouses or children of veterans or wage earners

eligible for social security payments. The recommended baseline categorization of the survivor compensation information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.15.5.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of survivor compensation information on the ability of responsible agencies to provide compensation to the survivors of individuals currently receiving or eligible to receive benefits from the Federal Government. The consequences of unauthorized disclosure of most survivor compensation information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in training and employment systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals).

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for survivor compensation information is ***low***.

D.15.5.2 Integrity

The consequences of unauthorized modification to or destruction of survivor compensation information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. A more serious threat may be that of modification of access control information or mechanisms in order to gain access to privacy information may have significant adverse effects on operations and/or public confidence in the agency, but the damage to the mission would again usually be limited and can generally be corrected within reasonable time and resource constraints. Another threat is that of unauthorized modification of information in order to perpetrate fraud (e.g., creation of false accounts or diversion of payments). This might result in harm to individuals, but fraud on a scale likely to do serious harm to agency operations or missions should be detected by monitoring and audit processes.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most survivor compensation information is ***low***.

D.15.5.3 Availability

The effects of disruption of access to or use of most survivor compensation information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for survivor compensation information is ***low***.

D.16 Law Enforcement

Law enforcement involves the protection of people, places, and things from criminal activity resulting from non-compliance with U.S. laws. This includes patrols, undercover operations, response to emergency calls, as well as arrests, raids, and seizures of property. Note that impacts to some information and information systems associated with law enforcement missions may affect the security of a broad range of critical infrastructures and key national assets. Note also that some information associated with Federal law enforcement is categorized as *national security information*. Rules governing establishment of impact levels and controls associated with *national security information* are governed by a separate set of policies and are outside the scope of this guideline.

D.16.1 Criminal Apprehension Information Type

Criminal apprehension supports activities associated with the tracking and capture of groups or individuals believed to be responsible of committing Federal crimes. The recommended baseline categorization of the criminal apprehension information type follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, MODERATE), (**availability**, HIGH)}

D.16.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of criminal apprehension information on the ability of responsible agencies to track and capture groups or individuals believed to be responsible for committing Federal crimes, on public safety, and on the safety of law enforcement officers. The consequences of unauthorized disclosure of criminal apprehension information depend 1) on the seriousness of the crime involved, 2) on the capability and predisposition of the criminal to injure or kill civilians or law enforcement officials, and 3) timing (e.g., the ability of the targeted criminal entity to access the information and use it to facilitate a criminal enterprise or to evade capture). The ability of a criminal entity to access and use information which has been disclosed without authorization (as a result of intent or negligence) is often dependent on the level of sophistication and/or the magnitude of resources available to that criminal entity. This is particularly so when the unauthorized disclosure takes the form of a vulnerability to intercept of transmitted information or intrusion into data repositories rather than of unauthorized distribution.

Special Factors Affecting Confidentiality Impact Determination: In cases where 1) the crimes are not violent and do not involve extraordinarily large property losses, and 2)

there is no indication of a record of or predisposition to violence on the part of the criminal entity, the confidentiality impact may be ***low*** or ***moderate.***

Recommended Confidentiality Impact Level: Given the nature of many of the crimes that are the responsibility of Federal law enforcement agencies, the consequences associated with unauthorized disclosure of criminal apprehension information must often be assumed to pose a threat to human life or result in a loss of major assets. Therefore, the default confidentiality impact recommended for criminal apprehension information is ***high***.

D.16.1.2 Integrity

The consequences of unauthorized modification to or destruction of criminal apprehension information depends, on mitigating procedures and controls, on the urgency with which the information is needed, and on the effect which unauthorized modification or destruction of any instantiation of the information can be expected to have on the success of subsequent prosecution of the apprehended criminal(s). The consequences of unauthorized modification or destruction of much criminal apprehension information can generally be overcome if basic mitigating procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In many of these cases, the integrity impact level associated with criminal apprehension information is ***low***. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. In this case too, the integrity impact level recommended for criminal apprehension information is ***low***.

Special Factors Affecting Integrity Impact Determination: Where unauthorized modification or destruction of any instantiation of the information can be expected to have an adverse effect on the success of subsequent prosecution of the apprehended criminal (e.g., breaking the chain of evidence), a serious adverse effect on agency operations can result. This can place the agency at a significant disadvantage. In such cases, the integrity impact level recommended for criminal apprehension information is at least ***moderate***. Criminal apprehension mission requirements may not permit sufficient time to recognize anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives. Examples include modification of the address on a no knock warrant, modification of the number of suspects in an armed felony pursuit situation from several to one, and modification of a tactical assignment to omit reference to a hostage, high explosive, or dependent child. In such cases, unauthorized modification or destruction of information affecting criminal apprehension information may be expected to have a severe or catastrophic effect on public confidence in the agency, pose a significant threat to major assets, and/or pose a threat to human life. Given the nature of many of the crimes that are the responsibility of Federal law enforcement agencies, where there is a reasonable potential for modified

information to be acted upon in a tactical situation, the integrity impact level recommended for criminal apprehension information is ***high***.

Recommended Integrity Impact Level: In the general case, where there is a low probability that modified information will be acted on in a tactical situation, the default integrity impact level recommended for criminal apprehension information is ***moderate***.

D.16.1.3 Availability

The effects of disruption of access to or use of criminal apprehension information or information systems cannot be depended upon to be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, and the nature of missions supported by criminal apprehension information are not reliably tolerant of delay. Basic procedures and controls, such as alternate communications media, are often needed to prevent significant degradation in mission capability and resultant serious or catastrophic consequences. While there are many cases in which elements of criminal apprehension information are not urgent, there are many in which relatively short periods of unavailability can pose a threat to human life and/or result in a loss of major assets.

Recommended Availability Impact Level: The default availability impact level recommended for criminal apprehension information is ***high***.

D.16.2 Criminal Investigation and Surveillance Information Type

Criminal investigation and surveillance includes the collection of evidence required to determine responsibility for a crime and the monitoring and questioning of affected parties. The recommended baseline categorization of the criminal investigation and surveillance information type follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, MODERATE), (**availability**, MODERATE)}

D.16.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of criminal investigation and surveillance information on the ability of responsible agencies to collect evidence required to determine responsibility for a crime, to monitor and question affected parties, and to protect the safety of witnesses and law enforcement officers. The consequences of unauthorized disclosure of criminal investigation and surveillance information depend 1] on the seriousness of the crime involved, 2] timing (e.g., the ability of the targeted criminal entity[23] to access the information and use it to facilitate a criminal enterprise, to evade detection or surveillance, or eliminate probable cause for searches and warrants), and 3] on the capability and predisposition of the criminal to injure or witnesses or law enforcement officials critical to building a winnable case for the prosecution. The ability of a criminal entity to access and use information which has been disclosed without authorization (as a result of intent or negligence) is often dependent on the level of sophistication and/or the magnitude of resources available to

[23] In this case, the term "criminal entity" includes both the criminal and legal representative(s) of the criminal (i.e., council).

that criminal entity. This is particularly so when the unauthorized disclosure takes the form of a vulnerability to intercept of transmitted information or intrusion into data repositories rather than of unauthorized distribution.

Special Factors Affecting Confidentiality Impact Determination: In cases where 1) the crimes are not violent and do not involve extraordinarily large property losses, and 2) there is no indication of a record of or predisposition to violence on the part of the criminal entity, the confidentiality impact may be ***low*** or ***moderate***. Given the nature of many of the crimes that are the responsibility of Federal law enforcement agencies, the consequences associated with unauthorized disclosure of criminal investigation and surveillance information must often be assumed to pose a threat to human life or result in a loss of major assets. Additionally, when it concerns matters of trans-national interest, such as trade enforcement, tariff agreements, etc., or where foreign nationals might be involved, the confidentiality risk will be ***high***. Information that reveals the identity and/or location of informants may be of particular concern.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for criminal investigation and surveillance information is ***high***.

D.16.2.2 Integrity

The consequences of unauthorized modification to or destruction of criminal investigation and surveillance information depends, on mitigating procedures and controls, on the urgency with which the information is needed, and on the effect which unauthorized modification or destruction of any instantiation of the information can be expected to have on the success of subsequent prosecution of the apprehended criminal(s). The consequences of unauthorized modification or destruction of much criminal investigation and surveillance information can be overcome if basic mitigating procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In many of these cases, the integrity impact level associated with criminal investigation and surveillance information is ***low***. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. In this case too, the integrity impact level recommended for criminal investigation and surveillance information is ***low***.

Special Factors Affecting Integrity Impact Determination: Where unauthorized modification or destruction of any instantiation of the information can be expected to have an adverse effect on the granting or execution of a search or wiretap warrant or on the success of subsequent prosecution of the apprehended criminal (e.g., breaking the chain of evidence), a serious adverse effect on agency operations can result. This can place the agency at a significant disadvantage. In such cases, the integrity impact level recommended for criminal investigation and surveillance information is at least ***moderate***. Criminal investigation and surveillance mission requirements may not permit sufficient time to recognize anomalous information and compare suspect information to

that contained in source material, back-up files, and/or archives (e.g., the case of warrants authorizing surveillance of significant events). In such cases, major investigations can be jeopardized. Where the criminal case under investigation involves major property losses, large scale financial frauds that have serious implications for financial markets, pose a threat to key national assets, or pose a threat to human life, the integrity impact level recommended for criminal investigation and surveillance information is ***high***. Likewise, where it concerns international matters, such as trade enforcement, tariff agreements, etc., or where foreign nationals might be involved, the integrity risk level for criminal investigation and surveillance information will be ***high***, since any deliberate or inadvertent corruption of such information could easily result in catastrophic adverse effects on future operations, individual reputations, or agency image, not to mention personal hazard.

Recommended Integrity Impact Level: In the general case, the default integrity impact level recommended for criminal investigation and surveillance information is ***moderate***.

D.16.2.3 Availability

The effects of disruption of access to or use of criminal investigation and surveillance information or information systems cannot be depended upon to be repaired in time to prevent loss of surveillance or arrest opportunities. While the time frame required for repair is dependent on mitigating procedures and controls, the nature of missions supported by criminal investigation and surveillance information are not always tolerant of delay. Basic procedures and controls, such as use of alternate communications media, are often needed to prevent significant degradation of surveillance operations and resultant serious consequences for ongoing investigations.

Special Factors Affecting Availability Impact Determination: While there are many cases in which elements of criminal investigation and surveillance information are not urgent, there are many in which relatively short periods of unavailability can result in lost surveillance opportunities or opportunities to use information in time to prevent a crime or permit an arrest. Where the crimes involved pose a threat to human life and/or result in a loss of major assets, the availability impact level recommended for criminal investigation and surveillance information is ***high***.

Recommended Availability Impact Level: In the general case, the default availability impact level recommended for criminal investigation and surveillance information is ***moderate***.

D.16.3 Citizen Protection Information Type

Citizen protection involves all activities performed to protect the general population of the United States from criminal activity. The following security categorization is recommended for the citizen protection information type:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, MODERATE, (**availability**, HIGH)}

D.16.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of citizen protection information on the ability of responsible agencies to protect the general population of the United States from criminal activity. In some cases, the nature of the criminal activity against which protection is being provided is terrorist activity intended to cause mass casualties. While the results of unauthorized disclosure of most citizen protection information are unlikely to have a serious adverse effect on agency operations, the exceptions can have catastrophic consequences.

Special Factors Affecting Confidentiality Impact Determination: One situation in which the consequences of unauthorized disclosure of citizen protection information could be severe presupposes availability of detailed intelligence information regarding a planned terrorist act. If a comprehensive set of Federal defensive dispositions became known to the terrorists, the terrorists might succeed in countering the citizen protection measures and carry out a devastating attack. The confidentiality impacts associated with information concerning defensive dispositions would, therefore be ***high***. While the adverse effects of unauthorized disclosure of some citizen protection information on law enforcement operations, assets, and individuals are limited; the stakes are usually higher. Federal citizen protection activities often seek to protect the public against life-threatening situations or against loss of major assets.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most citizen protection information is at least ***moderate***.

D.16.3.2 Integrity

The consequences of unauthorized modification or destruction of citizen protection information can be serious if its nature and timing results in even momentary weaknesses on the protective measures. In many cases, competent agency personnel should be able to recognize anomalous information (e.g., by recognizing orders as suspect and reconfirming using call-back mechanisms). Damage can generally be corrected within reasonable time and resource constraints, but there is a substantial potential threat to public safety in the interim.

Special Factors Affecting Integrity Impact Determination: In some cases (e.g., terrorist threats), unauthorized modification or destruction of citizen protection information can result in loss of human life - a ***high***-impact potential.

Recommended Integrity Impact Level: In general, the default integrity impact level recommended for citizen protection information is ***moderate***.

D.16.3.3 Availability

The effects of disruption of access to or use of citizen protection information or information systems can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Many citizen protection missions are usually tolerant of reasonable delays.

Special Factors Affecting Availability Impact Determination: Emergency situations or elevated terrorist threat conditions are not tolerant of delays.

Recommended Availability Impact Level: In view of the need to be able to conduct time-sensitive operations aimed at life-threatening situations, the default availability impact level recommended for citizen protection information is normally ***high***.

D.16.4 Leadership Protection Information Type

Leadership protection involves all activities performed to protect the health and well being of the president, vice-president, their families, and other high-level government officials. Some leadership protection information may be classified. All classified information is treated under separate rules established for *national security information* and is outside the scope of this guideline. The recommended categorization for unclassified leadership protection information follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, HIGH), (**availability**, HIGH)}

D.16.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of leadership protection information on the abilities of responsible agencies to protect the health and well being of the president, vice-president, their families, and other high-level government officials. The consequences of unauthorized disclosure of leadership protection information can, not only pose a threat to human life, but in extreme cases can have a disruptive effect on the continuity of Federal government operations.

Recommended Confidentiality Impact Level: Given the criticality of much leadership protection information, and the severe or catastrophic consequences to agencies that can result from disclosure of leadership protection information without proper authorization, the default confidentiality impact level recommended for the information is generally ***high***.

D.16.4.2 Integrity

The consequences of unauthorized modification or destruction of leadership protection information is determined to a large extent on the specific operation(s) supported by the information. Also, the consequences of unauthorized modification or destruction of leadership protection information generally depends less on mitigating procedures and controls than on the urgency with which the intelligence information is needed. Operational requirements may not permit sufficient time to recognize anomalous information and/or compare suspect information to that contained in source materials. Unauthorized modification or destruction of information affecting leadership protection information may adversely affect mission operations in a manner that results in loss of human life and disruption of government operations.

Recommended Integrity Impact Level: The integrity impact level recommended for leadership protection information is normally ***high***.

D.16.4.3 Availability

The effects of disruption of access to or use of leadership protection information or information systems cannot necessarily be repaired in time to prevent catastrophic loss (e.g., threat warning information). The time frame required for repair is dependent on mitigating procedures and controls, but the nature of missions supported by leadership protection information is not reliably tolerant of delays. Basic procedures and controls, such as alternate communications media and retention of copies of source material, cannot be depended on to prevent significant degradation in mission capability and resultant catastrophic consequences for mission capability and human life.

Recommended Availability Impact Level: The default availability impact level recommended for leadership protection information is ***high***.

D.16.5 Property Protection Information Type

Property protection entails all activities performed to ensure the security of civilian and government property. The recommended baseline categorization of the property protection information type follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, MODERATE)}

D.16.5.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of property protection information on the ability of responsible agencies to ensure the security of civilian and government property. The consequences of unauthorized disclosure of property protection information are generally dependent on the nature of the property being protected. Where the property being protected involves particularly sensitive classified information, the property protection information itself might be classified. In many cases in which the protected property involves command and control and other military facilities, foreign intelligence collection or processing facilities, weapons or weapons facilities, or cryptologic activities related to national security, property protection information is likely to be designated *national security information*, whether or not it is classified. *National security information* is outside the scope of this guideline. Where the property being protected is neither critical to agency operations or of such value that its loss would degrade mission capability or place the agency at a significant disadvantage, unauthorized disclosure would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. In such cases, the associated confidentiality impact would be ***low***.

Special Factors Affecting Confidentiality Impact Determination: Where critical infrastructure facilities or key national assets are being protected, the consequences of unauthorized disclosure of property protection information might reveal vulnerabilities in protection measures to terrorists or other adversaries. Such information may reveal to an enemy the most effective technique(s) or approach(es) to use in attacking a target, and/or assumptions on the part of defensive organizations regarding the capabilities, intent, and plans of our adversaries. Where unauthorized disclosure of property protection information associated with critical infrastructures, large groups of people, or key

national assets is expected to be of direct use to terrorists, the confidentiality impact level is assumed to be ***high***. Most protected facilities don't fall into *national security*, low value/criticality, critical infrastructure, or key national asset categories. If unauthorized disclosure of property protection information resulted in damage to or loss of these facilities, serious adverse effects on agency operations and agency assets could reasonably be expected to result.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for most property protection information is ***moderate***.

D.16.5.2 Integrity

The consequences of unauthorized modification to or destruction of property protection information depends, not only on the nature of the property being protected, but also on the immediacy with which the information is expected to be used. The consequences of unauthorized modification or destruction of property protection information can generally be overcome if basic mitigating procedures and controls implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the potential damage to the protection mission would usually be of more immediate concern. If the modified or destroyed information is tactical in nature, there is a greater potential for actions being taken based on incomplete or false information. This can have serious adverse effects on protection operations with consequent damage to, loss of, or other unauthorized access to property. The severity of the consequent integrity impact depends on the nature of the property (see D.16.5.1), but would be most likely to be ***moderate***.

Recommended Integrity Impact Level: The recommended default integrity impact level for property protection information is ***moderate***.

D.16.5.3 Availability

The effects of disruption of access to or use of property protection information or information systems cannot necessarily be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of missions supported by property protection information is not reliably tolerant of delays. The consequences of inability of guard forces and other emergency responders to receive threat information in a timely manner or to coordinate effectively with each other can result in complete mission failure and collateral damage to individuals. Basic mitigating procedures and controls cannot be depended on to prevent significant degradation in mission capability and resultant catastrophic consequences for properties that could include critical infrastructures and key national assets. In general, the availability impact level assigned to property protection information is dependent on what is being protected.

Recommended Availability Impact Level: The default availability impact recommended for most property protection information is ***moderate.***

D.16.6 Substance Control Information Type

Substance control supports activities associated with the enforcement of legal substances (i.e., alcohol and tobacco) and illegal narcotics laws including trafficking, possession, sale, distribution, and other related activities. The default security categorization recommended for the substance control information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, HIGH), (**availability**, LOW)}

D.16.6.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of substance control information on the ability of responsible agencies to enforce legal substances (i.e., alcohol and tobacco) and illegal narcotics laws including trafficking, possession, sale, distribution, and other related activities. Where the unauthorized disclosure of information expose sensitive information sources, or compromise investigative or interdiction operations, the consequences of unauthorized disclosure of substance control information may have a serious adverse effect on agency operations, significantly degrade mission capability, and/or pose a threat to human life. People and organizations involved in trafficking of narcotics and other illegal substances are frequently well funded, well organized, and/or pre-disposed to violence. The dollar values associated with these illegal activities are often very large. Where unauthorized disclosure endangers investigations in process, investigative or intelligence information sources, or information regarding witnesses or other critical case file elements, the danger to human life and key agency missions can be significant. Where unauthorized disclosure endangers witnesses or law enforcement officers, the impact level must be rated as ***high***. Other factors affecting confidentiality impacts associated with substance control information are discussed under Section D.16.1 (Criminal Apprehension) and Section D.16.2 (Criminal Investigation and Surveillance).

Special Factors Affecting Confidentiality Impact Determination: Some substance control information is classified, and other substance control information is tightly bound to *national security information* (e.g., intelligence information). Classified information and other *national security information* are outside the scope of this guideline. Unauthorized disclosure of some routine substance control information is highly unlikely to have more than a limited adverse effect on agency operations, agency assets, or individuals. The confidentiality impact associated with such information is ***low***. Unauthorized disclosure of a significant proportion of substance control information can compromise investigations, cause apprehension operations to fail, and compromise prosecutions. This can have a serious adverse effect on agency operations and place the agency at a significant disadvantage. Because of this, the confidentiality impact level associated with much substance control information is at least ***moderate.***

Recommended Confidentiality Impact Level: Because of the high stakes involved and the significant potential for loss of life resulting from compromise of substance control information, the recommended default confidentiality impact level is ***high***.

D.16.6.2 Integrity

Because of the very well funded nature of the narcotics trade, the variety of credible integrity threats is larger than for most criminal endeavors. The consequences of unauthorized modification or destruction of substance control information can sometimes be overcome if basic mitigating procedures and controls are implemented and used, but the amount of money available to perpetrators significantly increases the insider threat and complicates detection activities. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to most missions would usually be limited. Unauthorized modification or destruction of information affecting internal communications can jeopardize investigations, prosecutions, the lives of witnesses, and the safety of enforcement officers. In many cases, competent agency personnel may be able to recognize anomalous information and compare suspect information to that contained in source materials. However, there remains a significant probability that modification to or destruction of information will not be discovered until it is too late. Damage can generally be corrected within reasonable time and resource constraints, but there is a substantial potential threat to public safety in the interim. Other factors affecting integrity impacts associated with substance control information are discussed under Section D.16.1 (Criminal Apprehension) and Section D.16.2 (Criminal Investigation and Surveillance). In some cases, unauthorized modification or destruction of information can result in loss of human life. The consequences of unauthorized modification or destruction of information can be serious or catastrophic if its nature and timing results in modification of information critical to tactical operations (e.g., modification of an address on a search warrant). The consequences can be equally serious if the destruction or modification of information renders ineffective confidentiality mechanisms that protect high-impact information.

Recommended Integrity Impact Level: Because of the potential consequences to protection missions and associated life-threatening consequences, the default integrity impact level recommended for substance control information is ***high***.

D.16.6.3 Availability

The effects of disruption of access to or use of substance control information or information systems can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Except for cases of emergency communications and other emergency processes associated with apprehension or time-sensitive surveillance operations, most substance control processes are usually tolerant of reasonable delays. Use of basic procedures and controls, such as alternate communications media and retention of copies of key information, can generally prevent major compromise of mission capability.

Special Factors Affecting Availability Impact Determination: Failure of some processes during tactical operations can result in both threat to human life and severe harm to public confidence in the agency. The impact level assigned to information and information systems associated with these tactical processes is ***high***.

Recommended Availability Impact Level: The default availability impact level recommended for most substance control information is ***low***.

D.16.7 Crime Prevention Information Type

Crime prevention entails all efforts designed to create safer communities through the control and reduction of crime by addressing the causes of crime and reducing the opportunities of crime. The general recommended security categorization for the crime prevention information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.16.7.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of crime prevention information on the ability of responsible agencies to create safer communities through the control and reduction of crime by addressing the causes of crime and reducing the opportunities of crime.

Special Factors Affecting Confidentiality Impact Determination: In a very few cases, details of crime prevention programs are sensitive (e.g., location of actively monitored surveillance cameras where only a fraction of camera feeds are monitored). In such cases, unauthorized disclosure crime prevention information might have a serious adverse effect on crime prevention operations by eliminating uncertainty regarding surveillance patterns. In such cases, the confidentiality impact might be ***moderate***.

Recommended Confidentiality Impact Level: In the vast majority of cases, unauthorized disclosure of crime prevention information will have only a limited adverse effect on agency operations, assets, or individuals. Therefore, the default confidentiality impact level recommended for crime prevention information is ***low***.

D.16.7.2 Integrity

Crime prevention activities are not generally time-critical. The consequences of unauthorized modification of crime prevention information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In most cases, the adverse effects of unauthorized modification to or destruction of crime prevention information on agency mission functions and/or public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for crime prevention information is ***low***.

D.16.7.3 Availability

The effects of disruption of access to or use of crime prevention information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Most crime prevention processes are tolerant of delay.

Special Factors Affecting Availability Impact Determination: In exceptional cases (e.g., orders associated with deployment of officers to provide a crime-discouraging presence in developing threat situations like potentially violent protest demonstrations), loss of availability of information can have a serious adverse effect on crime prevention operations. In such cases, the availability impact might be ***moderate***. Basic procedures and controls, such as use of back-up files and alternate facilities, can usually prevent serious damage to mission capability. In most cases, disruption of access to or use of crime prevention information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: default availability impact recommended for crime prevention information is ***low***.

D.16.8 Trade Law Enforcement Information Type

Trade law enforcement refers to the enforcement of anti-boycott, international loan, and general trade laws. The security categorization recommended for the trade law enforcement information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, HIGH), (**availability**, HIGH)}

D.16.8.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of trade law enforcement information on the ability of responsible agencies to enforce various Customs laws. Unauthorized disclosure of trade law enforcement information could potentially jeopardize fulfillment of other trade law enforcement missions. Some information that has supported a trade law enforcement process might be of higher sensitivity, and unauthorized disclosure of such might jeopardize the success of future trade law enforcement processes. In the case of intelligence information, this falls under *national security systems. National security information* and *national security systems* are, by definition, outside the scope of this guideline. The consequent threat to agency image or reputations can cause a serious adverse effect on an agency's mission capability. Where information includes names of informants, personnel involved in informant contact, or involvement of agency personnel in specific prior activities, the effectiveness of those personnel in support of future enforcement activities can be permanently impaired, or those individuals could potentially be exposed to personal hazard.

Recommended Confidentiality Impact Level: The general confidentiality risk level recommended for trade law enforcement information is ***high***.

D.16.8.2 Integrity

The consequences of unauthorized modification or destruction of trade law enforcement information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is needed. The requirement for adequate means to detect data corruption is ***high***, since this information might potentially be evidence in legal proceedings. Unauthorized modification or destruction of information affecting trade law enforcement information may adversely affect mission operations in a manner that results in unacceptable consequences in terms of potential personnel hazard. Corruption of trade law enforcement information can be serious or catastrophic if its nature and timing results in modification of information critical to tactical operations. Additionally, once finalized, the results of trade law enforcement activities may become matters of public record, and thus are extremely critical in terms of being accurately recorded.

Recommended Integrity Impact Level: The default integrity risk level recommended for trade law enforcement information is ***high***.

D.16.8.3 Availability

The effects of disruption of access to or use of trade law enforcement information or information systems can be serious or catastrophic if its nature and timing results in modification of information critical to tactical operations. The time frame required for repair is dependent on mitigating procedures and controls, but the nature of trade law enforcement missions is quite intolerant of significant delays. Mission requirements will almost never allow sufficient time to restore access, rebuild files, and recognize anomalous information and compare suspect information to that contained in source materials before the information is used.

Recommended Availability Impact Level: The default availability risk level recommended for trade law enforcement information is ***high***.

D.17 Legal

Legal involves all activities necessary for the development and oversight of Federal programs.

D.17.1 Judicial Hearings Information Type

Judicial hearings include activities associated with conducting a hearing in a court of law to settle a dispute. The general recommended security categorization for the judicial hearings information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, LOW), (**availability**, LOW)}

D.17.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of judicial hearings information on the ability of responsible entities to conducting a hearing in a court of law to settle a dispute. While much information associated with judicial hearings is public, some information is sealed by the court and its unauthorized disclosure is

punishable by law by fine and/or imprisonment. Examples of sensitive information include informant information and hearsay evidence, but discretion for prohibition of disclosure generally rests with the judge. Where unauthorized disclosure of information might have a serious adverse effect on judicial hearings, the confidentiality impact might be ***moderate***. Where the life of a victim, witness, or informant may be endangered by disclosure, the confidentiality risk is ***high***. Also, where the consequences of a miscarriage of justice are likely to endanger public safety, the confidentiality risk is ***high***. In the vast majority of cases, unauthorized disclosure of judicial hearings information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: Given legal consequences of unauthorized disclosure and potential consequences for human life, the default confidentiality impact level recommended for judicial hearings information is ***high***.

D.17.1.2 Integrity

Judicial hearings activities are not generally time-critical. The consequences of unauthorized modification of judicial hearings information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. Modification or destruction of court records can result in disruption of or jeopardy to legal proceedings, but recovery of true copies can mitigate this threat. In most cases, the adverse effects of unauthorized modification to or destruction of judicial hearings information on agency mission functions and/or public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for judicial hearings information is ***low***.

D.17.1.3 Availability

The effects of disruption of access to or use of judicial hearings information can usually be repaired. The time frame required for repair is dependent on implementation and use of adequate back up information, facilities and procedures. Most judicial hearings processes are tolerant of delay.

Special Factors Affecting Availability Impact Determination: In exceptional cases (e.g., orders associated with wiretap or search warrants issued to prevent violent crime), loss of availability of information can have a serious or severe adverse effect. In such cases, the availability impact might be ***moderate*** or even ***high***. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious damage. In most cases, disruption of access to or use of judicial hearings information can be expected to have only a limited adverse effect on government operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for judicial hearings information is ***low***.

D.17.2 Legal Defense Information Type

Legal defense refers to the representation of a defendant in a criminal/civil court of law in an attempt to provide constitutional guarantees to legal representation. The general recommended security categorization for the legal defense information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, HIGH), (**availability**, LOW)}

D.17.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of legal defense information on the representation of a defendant in a criminal/civil court of law and on the ability of the government to provide constitutional guarantees to legal representation. Dissemination of legal defense information is governed, not only by privacy laws, but also by Rules of Criminal Procedure, Rules of Civil Procedure, and other laws governing adversarial legal proceedings. While much information associated with legal defense is public, some information is sealed by the court or is otherwise protected from disclosure. Violation of rules regarding unauthorized disclosure is punishable by law by disbarment, fine and/or imprisonment. Examples of sensitive information include informant information and incriminating information that is protected by the constitution or court rulings in constitutional law. Where unauthorized disclosure of information might have a serious adverse effect on legal defense, there is a presumption of a miscarriage of justice. If an unauthorized disclosure is discovered, the legal proceeding is jeopardized (e.g., a mistrial may be declared). The cost to the government and others in terms of finance, time, and disruption to normal operations can be severe. If suspicion is raised concerning government complicity in or negligence regarding unauthorized disclosure, serious loss of public confidence in government agencies or the legal process may result. In this case, the confidentiality impact of unauthorized disclosure is ***moderate***. Where the life of a victim, witness, or informant may be endangered by disclosure, the confidentiality risk is ***high***. Also, where the consequences of a miscarriage of justice are likely to endanger public safety (e.g., release of a terrorist or other murderer), the confidentiality risk is ***high***. In the vast majority of cases, unauthorized disclosure of legal defense information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: Given legal consequences of unauthorized disclosure and potential consequences for human life, the default confidentiality impact level recommended for legal defense information is ***high***.

D.17.2.2 Integrity

Legal defense activities are not generally time-critical. The consequences of unauthorized modification of legal defense information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. On the other hand, in the case of legal defense information, the fact that evidence or other defense information has been tampered with can jeopardize legal proceedings (e.g., a mistrial may be declared). The cost to the government and other entities in terms of finance, time, and disruption to normal operations can be severe. If suspicion is raised

concerning government complicity in or negligence regarding unauthorized modification or destruction of legal defense information, serious loss of public confidence in government agencies or the legal process may result. In this case, the confidentiality impact of unauthorized disclosure is ***moderate***. Where the life of a victim, witness, or informant may be endangered by disclosure, the confidentiality risk is ***high***. Also, where the consequences of a miscarriage of justice are likely to endanger public safety (e.g., release of a terrorist or other murderer), the confidentiality risk is ***high***. In any event, there is a significant probability that the modification or destruction will result in expensive and disruptive civil or criminal proceedings. In the vast majority of cases, unauthorized modification or destruction of legal defense information will have only a limited adverse effect on government operations, government assets, or individuals.

Recommended Integrity Impact Level: Given legal consequences of unauthorized modification or destruction and occasional potential consequences for human life, the default integrity impact level recommended for legal defense information is ***high***.

D.17.2.3 Availability

The effects of disruption of access to or use of legal defense information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Most legal defense processes are tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious damage. However, the delays can impact court schedules, cause significant taxpayer expense, and potentially jeopardize legal proceedings (see C17.2.2). In most cases, non-malicious disruption of access to or use of legal defense information can be expected to have only a limited adverse effect on government operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: In exceptional cases (e.g., information affecting a ruling regarding an impending execution), loss of availability of information can have a severe adverse effect. The consequent availability impact level would be ***high***.

Special Factors Affecting Availability Impact Determination: The default availability impact level recommended for legal defense information is ***low***.

D.17.3 Legal Investigation Information Type

Legal investigation supports activities associated with gathering information about a given party (government agency, citizen, corporation) that would be admissible in a court of law, in an attempt to prove guilt or innocence. The recommended baseline categorization of the legal investigation information type follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, MODERATE), (**availability**, MODERATE)}

D.17.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of legal investigation information on the ability of responsible agencies to gather information

about a given party (government agency, citizen, corporation) that would be admissible in a court of law, in an attempt to prove guilt or innocence. The consequences of unauthorized disclosure of legal investigation information depend 1] on the seriousness of the crime involved, 2] timing (e.g., the ability of the targeted criminal entity[24] to access the information and use it to facilitate a criminal enterprise, to evade detection or surveillance, or eliminate probable cause for searches and warrants), and 3] on the capability and predisposition of the criminal to injure or witnesses or law enforcement officials critical to building a winnable case for the prosecution. The ability of a criminal entity to access and use information which has been disclosed without authorization (as a result of intent or negligence) is often dependent on the level of sophistication and/or the magnitude of resources available to that criminal entity. This is particularly so when the unauthorized disclosure takes the form of a vulnerability to intercept of transmitted information or intrusion into data repositories rather than of unauthorized distribution. In cases where 1) the crimes are not violent and do not involve extraordinarily large property losses, and 2) there is no indication of a record of or predisposition to violence on the part of the criminal entity, the confidentiality impact may be ***low*** or ***moderate***.

Special Factors Affecting Confidentiality Impact Determination: Given the nature of many of the crimes that are the responsibility of Federal law enforcement agencies, the consequences associated with unauthorized disclosure of legal investigation information must often be assumed to pose a threat to human life or result in a loss of major assets. Additionally, when it concerns matters of trans-national interest, such as trade enforcement, tariff agreements, etc., or where foreign nationals might be involved, the confidentiality risk will be ***high***. Information that reveals the identity and/or location of informants may be of particular concern.

Recommended Confidentiality Impact Level: Given potentially serious to severe legal consequences of unauthorized disclosure and potential consequences for human life, the default confidentiality impact level recommended for legal defense information is ***high***.

D.17.3.2 Integrity

The consequences of unauthorized modification to or destruction of legal investigation information depends, on mitigating procedures and controls, on the urgency with which the information is needed, and on the effect which unauthorized modification or destruction of any instantiation of the information can be expected to have on the success of subsequent prosecution of the apprehended criminal(s). The consequences of unauthorized modification or destruction of much legal investigation information can be overcome if basic mitigating procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In many of these cases, the integrity impact level associated with legal investigation information is ***low***. Unauthorized modification or destruction of information affecting external communications associated with legal investigative organizations (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but

[24] In this case, the term "criminal entity" includes both the criminal and legal representative(s) of the criminal (i.e., council).

the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. In this case too, the integrity impact level recommended for legal investigation information is ***low***. Where unauthorized modification or destruction of any instantiation of the information can be expected to have an adverse effect on the granting or execution of a search or wiretap warrant or on the success of subsequent prosecution of the apprehended criminal (e.g., breaking the chain of evidence), a serious adverse effect on agency operations can result. This can place the agency at a significant disadvantage. In such cases, the integrity impact level recommended for legal investigation information is at least ***moderate***.

Special Factors Affecting Integrity Impact Determination: Legal investigation mission requirements may not permit sufficient time to recognize anomalous information and compare suspect information to that contained in source materials (e.g., the case of warrants authorizing surveillance of significant events). In such cases, major investigations can be jeopardized. Where the criminal case under investigation involves major property losses, large-scale financial frauds that have serious implications for financial markets, pose a threat to key national assets, or pose a threat to human life, the integrity impact level recommended for legal investigation information is ***high***. Likewise, where it concerns international matters, such as trade enforcement, tariff agreements, etc., or where foreign nationals might be involved, the integrity risk level for legal investigation information will be ***high***, since any deliberate or inadvertent corruption of such information could easily result in catastrophic adverse effects on future operations, individual reputations, or agency image, not to mention personal hazard.

Recommended Integrity Impact Level: In the general case, the default integrity impact level recommended for legal investigation information is ***moderate***.

D.17.3.3 Availability

The effects of disruption of access to or use of legal investigation information or information systems cannot be depended upon to be repaired in time to prevent loss of surveillance or arrest opportunities. While the time frame required for repair is dependent on mitigating procedures and controls, the nature of missions supported by legal investigation information are not always tolerant of delay. Basic procedures and controls, such as alternate communications media, are often needed to prevent significant degradation of surveillance operations and resultant serious consequences for ongoing investigations.

Special Factors Affecting Availability Impact Determination: Where the crimes involved pose a threat to human life and/or result in a loss of major assets, the availability impact level recommended for legal investigation information is ***high***.

Recommended Availability Impact Level: In the general case, the default availability impact level recommended for legal investigation information is ***moderate***.

D.17.4 Legal Prosecution/Litigation Information Type

Legal prosecution/litigation includes all activities involved with presenting a case in a legal proceeding both in a criminal or civil court of law in an attempt to prove guilt/responsibility. The general recommended security categorization for the legal prosecution/litigation information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, HIGH), (**availability**, LOW)}

D.17.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of legal prosecution/litigation information on the ability of responsible agencies to present a case in a legal proceeding either in a criminal or civil court of law in an attempt to prove guilt/responsibility. Dissemination of legal prosecution/litigation information is governed, not only by privacy laws, but also by Rules of Criminal Procedure, Rules of Civil Procedure, and other laws governing adversarial legal proceedings. While much information associated with legal prosecution/litigation is public, some information is sealed by the court or is otherwise protected from disclosure. Violation of rules regarding unauthorized disclosure is punishable by law by disbarment, fine and/or imprisonment. Examples of sensitive information include informant information and incriminating information that is protected by the constitution or court rulings in constitutional law. Where unauthorized disclosure of information might have a serious adverse effect on legal prosecution/litigation, there is a presumption of a miscarriage of justice. [Note that the impact of unauthorized disclosure of *national security information* is outside the scope of this guideline.] If an unauthorized disclosure is discovered, the legal proceeding is jeopardized (e.g., a mistrial may be declared). The cost to the government and others in terms of finance, time, and disruption to normal operations can be severe. If suspicion is raised concerning government complicity in or negligence regarding unauthorized disclosure, serious loss of public confidence in government agencies or the legal process may result. In this case, the confidentiality impact of unauthorized disclosure is ***moderate***. Where the life of a complainant, victim, witness, or informant may be endangered by disclosure, the confidentiality risk is ***high***. Also, where the consequences of a miscarriage of justice are likely to endanger public safety (e.g., release of a terrorist or other murderer), the confidentiality risk is ***high***. In criminal cases, the consequences of unauthorized disclosure of legal prosecution information are affected by 1] the seriousness of the crime involved, 2] timing (e.g., the ability of the targeted criminal entity to access the information and use it to facilitate a criminal enterprise, to evade detection or surveillance, or eliminate probable cause for searches and warrants), and 3] the capability and predisposition of the criminal to injure or witnesses or law enforcement officials critical to building a winnable case for the prosecution. The ability of a criminal entity[25] to access and use information which has been disclosed without authorization (as a result of intent or negligence) is often dependent on the level of sophistication and/or the magnitude of resources available to that criminal entity. This is particularly so when the unauthorized disclosure takes the form of a vulnerability to intercept of transmitted information or intrusion into data repositories rather than of

[25] In this case, the term "criminal entity" includes both the criminal and legal representative(s) of the criminal (i.e., council).

unauthorized distribution. In cases where 1) the crimes are not violent and do not involve extraordinarily large property losses, and 2) there is no indication of a record of or predisposition to violence on the part of the criminal entity, the confidentiality impact may be ***low*** or ***moderate***. Given the nature of many of the crimes that are the responsibility of Federal law enforcement agencies, the consequences associated with unauthorized disclosure of legal prosecution information must often be assumed to pose a threat to human life or result in a loss of major assets. Additionally, when a legal proceeding concerns matters of trans-national interest, such as trade enforcement, tariff agreements, etc., or where foreign nationals might be involved, the confidentiality risk will be ***high***. Information that reveals the identity and/or location of informants may be of particular concern. In the vast majority of cases, unauthorized disclosure of legal prosecution/litigation information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: Given legal consequences of unauthorized disclosure and potential consequences for human life, the default confidentiality impact level recommended for legal prosecution/litigation information is ***high***.

D.17.4.2 Integrity

Legal prosecution/litigation activities are not generally time-critical. The consequences of unauthorized modification of legal prosecution/litigation information can generally be overcome if review procedures are in place and mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. Unauthorized modification or destruction of information affecting external communications associated with legal prosecution/litigation organizations (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. In this case, the integrity impact level recommended for legal investigation information is ***low***. On the other hand, in the case of legal prosecution/litigation information, the fact that evidence or other defense information has been tampered with can jeopardize legal proceedings (e.g., a mistrial may be declared). This is especially likely if it can be reasonably argued that the chain of critical evidence has been broken. The cost to the government and other entities in terms of finance, time, and disruption to normal operations can be severe. If suspicion is raised concerning government complicity in or negligence regarding unauthorized modification or destruction of legal prosecution/litigation information, serious loss of public confidence in government agencies or the legal process may result (not to mention the jeopardy to the government's case). In this case, the confidentiality impact of unauthorized disclosure is ***moderate***. Where the life of a victim, witness, or informant may be endangered by disclosure, the confidentiality risk is ***high***. Also, where the consequences of a miscarriage of justice are likely to endanger public safety (e.g., release of a terrorist or other murderer), the confidentiality risk is ***high***. In any event, there is a significant probability that the modification or destruction will result in expensive and disruptive civil or criminal proceedings. In the vast majority of cases, unauthorized

modification or destruction of legal prosecution/litigation information will have only a limited adverse effect on government operations, government assets, or individuals.

Recommended Integrity Impact Level: Given legal consequences of unauthorized modification or destruction and occasional potential consequences for human life, the default integrity impact level recommended for legal prosecution/litigation information is ***high***.

D.17.4.3 Availability

The effects of disruption of access to or use of legal prosecution/litigation information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Most legal prosecution/litigation processes are tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious damage. However, the delays can impact court schedules, cause significant taxpayer expense, and potentially jeopardize legal proceedings (see C17.4.2).

Special Factors Affecting Availability Impact Determination: In exceptional cases (e.g., information affecting a ruling regarding an impending execution), loss of availability of information can have a severe adverse effect. Where the agency is likely to prosecute crimes that involve threats to human life and/or result in a loss of major assets, the availability impact level recommended for legal prosecution/litigation information is ***high***.

Recommended Availability Impact Level: In most cases, non-malicious disruption of access to or use of legal prosecution/litigation information can be expected to have only a limited adverse effect on government operations, agency assets, or individuals. Therefore, the default availability impact recommended for legal prosecution/litigation information is ***low***.

D.17.5 Resolution Facilitation Information Type

Resolution facilitation involves all activities outside of a court of law that may be used in an attempt to settle a dispute between two or more parties (government, citizen, corporation). The general recommended security categorization for the resolution facilitation information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, HIGH), (**integrity**, LOW), (**availability**, LOW)}

D.17.5.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of resolution facilitation information on the ability of responsible entities to settle a dispute between two or more parties (government, citizen, corporation) outside of a court of law. While some information associated with resolution facilitation is public, much of the information is private and/or proprietary. Unauthorized disclosure of such information can disrupt, extend, and/or defeat the dispute resolution process. The consequences of harm to the resolution facilitation process depend generally on the nature of the dispute.

Jeopardy to the resolution process will not usually involve threats to critical infrastructures, key national assets, or human life. However, in exceptional cases (e.g., plea bargaining undertaken to ensure the long-term incarceration of a murderer the conviction of whom is in doubt), human lives may be jeopardized by failure of the resolution facilitation process. Where large monetary amounts and/or violent crimes are involved, the confidentiality impact of unauthorized disclosure of resolution facilitation information might be ***moderate*** to ***high***. Additionally, when resolution facilitation concerns matters of trans-national interest, such as trade enforcement, tariff agreements, etc., or where foreign nationals might be involved, the confidentiality risk will be ***high***. In the vast majority of cases, unauthorized disclosure of resolution facilitation information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: Given legal consequences of unauthorized disclosure and potential consequences for human life, the default confidentiality impact level recommended for resolution facilitation information is ***high***.

D.17.5.2 Integrity

Resolution facilitation activities are not generally time-critical. The consequences of unauthorized modification of resolution facilitation information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives. Modification or destruction of court records can result in disruption of or jeopardy to legal proceedings, but recovery of true copies can mitigate this threat. In most cases, the adverse effects of unauthorized modification to or destruction of resolution facilitation information on agency mission functions and/or public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact level recommended for resolution facilitation information is ***low***.

D.17.5.3 Availability

The effects of disruption of access to or use of resolution facilitation information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Most resolution facilitation processes are tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious damage. In most cases, disruption of access to or use of resolution facilitation information can be expected to have only a limited adverse effect on government operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for resolution facilitation information is ***low***.

D.18 Correctional Activities

Correctional Activities involves all Federal activities that ensure the effective incarceration and rehabilitation of convicted criminals.

D.18.1 Criminal Incarceration Information Type

Criminal incarceration includes activities associated with the housing, custody and general care of criminals sentenced to serve time in penitentiaries. The following security categorization is recommended for the criminal incarceration information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

D.18.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of criminal incarceration information on the ability of responsible agencies to provide housing, custody, and general care for criminals sentenced to serve time in a Federal penitentiary. The consequences of unauthorized disclosure of most criminal incarceration information are unlikely to have a serious adverse effect on agency operations. The most serious adverse effects are likely to involve exposure of information that is proprietary to prisoner that can result in damaging publicity for an organization. (Note that unauthorized disclosure of some information can conceivably have serious impact on the status or resolution of appeal actions). The consequences of unauthorized disclosures may have an adverse effect on public confidence in the agency, and may include short-term staffing challenges for the agency.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most criminal incarceration information is normally ***low***.

D.18.1.2 Integrity

The consequences of unauthorized modification or destruction of criminal incarceration information can be serious if its nature and timing results in premature release of the criminal and consequent exposure of the public to predation, unjust retention of an individual in the prison system, or harm to a citizen's reputation or public confidence in the government due to exposure of incorrect damaging information (e.g., if altered data becomes public). In many cases, competent agency personnel should be able to recognize anomalous information (e.g., by recognizing information as suspect and re-testing or comparing suspect information to that contained in or re-derived from source material, back-up files, and/or archives). Damage can generally be corrected within reasonable time and resource constraints, but there is a substantial potential threat to justice and/or public safety in the interim.

Special Factors Affecting Integrity Impact Determination: In some cases (e.g., instructions regarding a need to isolate a prisoner from the general prison population for personal safety reasons), unauthorized modification or destruction of criminal incarceration information can result in loss of human life - a ***high***-impact potential.

Recommended Integrity Impact Level: In general, the default integrity impact level recommended for criminal incarceration information is ***moderate.***

D.18.1.3 Availability

The effects of disruption of access to or use of criminal incarceration information or information systems can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Except for cases of emergency bulletins necessary to cope with health or safety threats to prisoners, the nature of criminal incarceration processes is usually tolerant of reasonable delays. Use of basic procedures and controls, such as alternate communications media and retention of copies of source material, can generally prevent major compromise of mission capability.

Special Factors Affecting Availability Impact Determination: There may be cases (e.g. emergency bulletins affecting prisoner health and/or safety) in which emergency dissemination of information regarding life-threatening situations is delayed for excessive periods. Such cases can result in a ***high*** availability impact level.

Recommended Availability Impact Level: Generally, the default availability impact level recommended for criminal incarceration information is ***low***.

D.18.2 Criminal Rehabilitation Information Type

Criminal Rehabilitation includes all government activities devoted to providing convicted criminals with the educational resources and life skills necessary to rejoin society as responsible and contributing members. The recommended baseline categorization of the criminal rehabilitation information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.18.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of criminal rehabilitation information on the ability of responsible agencies to provide convicted criminals with the educational resources and life skills necessary to rejoin society as responsible and contributing members. The consequences of unauthorized disclosure of most criminal rehabilitation information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Exceptions that might have a potential for more serious consequences are based on privacy information processed in criminal rehabilitation systems (e.g., information required by the Privacy Act of 1974 or other statutes and executive orders to receive special handling to protect the privacy of individuals).

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for criminal rehabilitation information is ***low***.

D.18.2.2 Integrity

The consequences of unauthorized modification to or destruction of criminal rehabilitation information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. Modification of access control information or mechanisms in order to gain access to privacy information may have significant adverse effects on operations and/or public confidence in the agency, but the damage to the mission would again usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most criminal rehabilitation information is ***low***.

D.18.2.3 Availability

The effects of disruption of access to or use of most criminal rehabilitation information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for criminal rehabilitation information is ***low***.

D.19 General Services and Information

General Science and Innovation includes all Federal activities to meet the national need to advance knowledge in this area. This includes general research and technology programs, space exploration activities, and other research and technology programs that have diverse goals and cannot be readily classified into another mission area or information type.

D.19.1 Scientific and Technical Research and Innovation Information Type

Scientific Innovation includes all federal activities whose goal is the creation of new scientific and/or technological knowledge as a goal in itself, without a specific link to the other mission areas or information types identified in the OMB Business Reference Model. While some information associated with scientific and technical research and innovation is *national security information*, most of that most sensitive information is being developed under research and development programs that directly support another of the mission areas described in this Appendix and are not included here. The recommended baseline categorization of information recommended for the scientific and technical research and innovation information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

D.19.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of scientific and technical research and innovation information on the ability of responsible agencies to create new scientific and/or technological knowledge as a goal in itself, without a specific link to the other program areas or information types. Many scientific and technical research and innovation activities are conducted in association with public institutions of higher learning, and the findings resulting from those activities are intended for publication.

Special Factors Affecting Confidentiality Impact Determination: Considerations associated with competition for funding and recognition (e.g., grants, development contract, patent rights, and copyrights) suggest that pre-publication disclosure or other unauthorized disclosure of can have a serious adverse effect on agency operations, agency assets, or individuals. In such cases, the confidentiality impact associated with information associated with scientific and technical research and innovation is ***moderate***. In some cases, the information associated with scientific and technical research and innovation is classified or otherwise qualified as *national security information*. Such information is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most information associated with scientific and technical research and innovation is ***low***.

D.19.1.2 Integrity

The consequences of unauthorized modification to or destruction of most information associated with scientific and technical research and innovation can be seriously disruptive to the progress of research activities. While basic procedures and controls (e.g., review procedures that include comparisons of current versions to previous versions) can often lead to timely discovery of and mitigation of the effects of integrity breaches, discovery may come too late to prevent disruption of research activities. This can result in serious consequences in terms of cost and institutional and/or public confidence in the affected organization. The effects on future funding can be quite serious and can have a serious adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be more limited and can generally be corrected within reasonable time and resource constraints. Modification of access control information or mechanisms in order to gain access to confidential information may have significant adverse confidentiality effects.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most information recommended for scientific and technical research and innovation is ***moderate***.

D.19.1.3 Availability

The effects of disruption of access to or use of most information associated with scientific and technical research and innovation can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Most research processes are tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious damage. In most cases, disruption of access to or use of research and innovation information can be expected to have only a limited adverse effect on government operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for information recommended for scientific and technical research and innovation is ***low***.

D.19.2 Space Exploration and Innovation Information Type

Space Exploration and Innovation includes all activities devoted to innovations directed at human and robotic space flight and the development and operation of space launch and transportation systems, and the general research and exploration of outer space. While some space exploration and innovation is *national security information*, most of that most sensitive information is being developed under research and development programs that directly support another of the mission areas described in this Appendix and are not included here. The recommended baseline categorization of the research and development information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

D.19.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of space exploration and innovation information on the ability of responsible agencies to conduct activities devoted to [1] innovations directed at human and robotic space flight and the development and operation of space launch and transportation systems, and [2] the general research and exploration of outer space. Many space exploration and innovation activities are conducted in association with public institutions of higher learning, and the findings resulting from those activities are intended for publication.

Special Factors Affecting Confidentiality Impact Determination: Considerations associated with competition for funding and recognition (e.g., grants, development contract, patent rights, and copyrights) suggest that pre-publication disclosure or other unauthorized disclosure of space exploration and innovation information can have a serious adverse effect on agency operations, agency assets, or individuals. In such cases, the confidentiality impact associated with space exploration and innovation is ***moderate***. In some cases, the space exploration and innovation information is classified or otherwise qualifies as *national security information* (e.g., where the information can assist a foreign power to develop weapons systems that endanger the national security of the United States). Such information is outside the scope of this guideline.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most space exploration and innovation information is ***low***.

D.19.2.2 Integrity

The consequences of unauthorized modification to or destruction of most space exploration and innovation information can be seriously disruptive to the progress of research activities. While use of basic procedures and controls can often lead to timely discovery of and mitigation of the effects of integrity breaches, discovery may come too late to prevent disruption of research activities. This can result in serious consequences in terms of cost and institutional and/or public confidence in the affected organization. The effects on future funding can be quite serious and can have a serious adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be more limited and can generally be corrected within reasonable time and resource constraints. Modification of access control information or mechanisms in order to gain access to confidential information may have significant adverse confidentiality effects.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most space exploration and innovation information is ***moderate***.

D.19.2.3 Availability

The effects of disruption of access to or use of most space exploration and innovation information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Most research and innovation processes are tolerant of delay. Basic procedures and control, such as availability and use of back-up files and alternate facilities, can usually prevent serious damage. In most cases, disruption of access to or use of research and innovation information can be expected to have only a limited adverse effect on government operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for space exploration and innovation information is ***low***.

D.20 Knowledge Creation and Management

Knowledge Creation and Management involves the programs and activities in which the Federal Government creates or develops a body or set of knowledge, the manipulation and analysis of which can provide inherent benefits for both the Federal and private sector.

D.20.1 Research and Development Information Type

Research and Development involves the gathering and analysis of data, dissemination of results, and development of new products, methodologies, and ideas. The sensitivity and criticality of most research and development information depends on the subject matter

involved. The recommended baseline categorization of the research and development information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

D.20.1.1 Confidentiality

The confidentiality impact level depends, not just on the effect of unauthorized disclosure of research and development information on the ability of responsible agencies to gather and analyze data, disseminate results, and develop new products, methodologies, and ideas, but also on the degree to which unauthorized disclosure of the information can assist hostile institutions to do harm to the interests of the government of the United States. Many research and development activities are conducted in association with public institutions of higher learning, and the findings resulting from those activities are intended for publication.

Special Factors Affecting Confidentiality Impact Determination: Considerations associated with competition for funding and recognition (e.g., grants, development contract, patent rights, and copyrights) suggest that pre-publication disclosure or other unauthorized disclosure of research findings can have a serious adverse effect on agency operations, agency assets, or individuals. In such cases, the confidentiality impact associated with research and development is ***moderate***. In some cases, the research and development information is classified or otherwise qualifies as *national security information* (e.g., where the information can assist a foreign power to develop weapons systems that endanger the national security of the United States). Such information is outside the scope of this guideline. Premature and/or partial release of preliminary research and development information can lead to misleading conclusions by policy makers, funding entities, news organizations, and/or the general public. These misleading conclusions can lead to termination of or other harm to the research and development projects. Where the research and development activities are associated with security measures or law enforcement tools, potential adversaries may derive insights that permit a head start on countermeasures development. In extreme cases, the resulting confidentiality impact can be ***high***.

Recommended Confidentiality Impact Level: Unauthorized disclosure of most research and development information can be expected to have only limited adverse effect on agency operations, agency assets, or individuals. Consequently, the default confidentiality impact level recommended for most government research and development information is ***low***.

D.20.1.2 Integrity

The consequences of unauthorized modification to or destruction of most research and development information can be seriously disruptive to the progress of research activities. While use of basic procedures and controls can often lead to timely discovery of and mitigation of the effects of integrity breaches, discovery may come too late to prevent disruption of research activities. This can result in serious consequences in terms of cost and institutional and/or public confidence in the affected organization. The effects on

future funding can be quite serious and can have a serious adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be more limited and can generally be corrected within reasonable time and resource constraints. Modification of access control information or mechanisms in order to gain access to confidential information may have significant adverse confidentiality effects.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most research and development information is ***moderate***.

D.20.1.3 Availability

The effects of disruption of access to or use of most research and development information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Most research and innovation processes are tolerant of delay. Basic procedures and control, such as availability and use of back-up files and alternate facilities, can usually prevent serious damage. In most cases, disruption of access to or use of research and innovation information can be expected to have only a limited adverse effect on government operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for research and development information is ***low***.

D.20.2 General Purpose Data and Statistics Information Type

General Purpose Data and Statistics includes activities performed in providing empirical, numerical, and related data and information pertaining to the current state of the nation in areas such as the economy, labor, weather, international trade, etc. The recommended baseline categorization of the general purpose data and statistics information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.20.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of general purpose data and statistics information on the ability of responsible agencies to provide empirical, numerical, and related data and information pertaining to the current state of the nation in areas such as the economy, labor, weather, international trade, etc. The consequences of unauthorized disclosure of most general-purpose data and statistics information would have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized premature disclosure of much economic (e.g., agricultural commodity, economic indicators) data and statistics information can result in major financial consequences. In

some cases, premature disclosure of this information can impact major financial markets and damage national banking and finance infrastructures. For example, unauthorized and premature disclosure of crop predictions by the Department of Agriculture can have a dramatic effect on commodity markets, with further consequences for financial markets in general. Unauthorized and premature disclosure to a single institution (e.g., a major commodity brokerage house), could damage faith in general purpose data and statistics gathering and development institutions, result in even more market disruption, and have a severe or catastrophic adverse effect on public confidence in the agency. Even where the consequences are limited to giving an unfair market advantage to a single financial or commercial institution, unauthorized disclosure can have a serious adverse effect on public confidence in the agency and its staff. One may postulate scenarios in which unauthorized disclosure might have a catastrophic effect on national financial/economic institutions, thus creating a ***high*** confidentiality impact. However, the conditions required to create or facilitate, then exploit such scenarios are generally improbable and/or elaborate.

Recommended Confidentiality Impact Level: The recommended default confidentiality impact level for most general purpose data and statistics information is ***low.***

D.20.2.2 Integrity

The consequences of unauthorized modification to or destruction of general purpose data and statistics information depends, not only on mitigating procedures and controls, but on the urgency with which the information is normally needed. The consequences of unauthorized modification or destruction of general purpose data and statistics information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives.

Special Factors Affecting Integrity Impact Determination: Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints. There may be on-line, automated, or semi-automated activities for which integrity threats can be realized before they are detected. Procedures are in place in most Federal general-purpose data and statistics institutions to mitigate the effects of these consequences. Where unauthorized modification or destruction of general purpose data and statistics information facilitates or enables a catastrophic confidentiality or availability impact scenario, the integrity impact level may be ***high***.

Recommended Integrity Impact Level: The default integrity impact level recommended for most modification or destruction of most general purpose data and statistics information is ***low***.

D.20.2.3 Availability

The effects of disruption of access to or use of general purpose data and statistics information or information systems can usually be repaired in time to prevent catastrophic loss. The time frame required for repair is dependent on mitigating procedures and controls, and the nature of missions supported by general-purpose data and statistics information is generally tolerant of delay. Basic procedures and controls, such as alternate communications media and retention of copies of source material, can usually be depended on to prevent significant degradation in mission capability and resultant serious or catastrophic consequences.

Special Factors Affecting Availability Impact Determination: There are circumstances under which a period of unavailability can be long enough to shake the confidence financial markets place in government institutions.

Recommended Availability Impact Level: The default availability impact level recommended for general purpose data and statistics information is ***low***.

D.20.3 Advising and Consulting Information Type

Advising and Consulting activities involve the guidance and consultative services provided by the Federal Government to support the implementation of a specific service provided to citizens. The recommended baseline categorization of the advising and consulting information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.20.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of advising and consulting information on the ability of responsible agencies to provide guidance and consultative services to support the implementation of a specific service to citizens. The consequences of unauthorized disclosure of advising and consulting information depends on the nature of the service being provided and on the sensitivity of the information with which advisory or consulting entities are working. The consequences of unauthorized disclosure of most advising and consulting information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where consulting support involves classified or other *national security information*, the consequences of unauthorized disclosure can be severe but are outside the scope of this guideline. In other cases, such as consultative services provided to law enforcement institutions, the consequences of unauthorized disclosure can be serious or even life threatening.

Recommended Confidentiality Impact Level: The default confidentiality impact recommended for advising and consulting information is ***low***.

D.20.3.2 Integrity

The consequences of unauthorized modification to or destruction of advising and consulting information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level associated with modification or destruction of most advising and consulting information is ***low***.

D.20.3.3 Availability

The effects of disruption of access to or use of most advising and consulting information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for advising and consulting information is ***low***.

D.20.4 Knowledge Dissemination Information Type

Knowledge Dissemination addresses those instances where the primary method used in delivering a service is through the publishing or broadcasting of information, such as the Voice of America or web-based museums maintained by the Smithsonian. It is not intended to address circumstances where the publication of information is a by-product of a mission rather than the mission itself. The recommended baseline categorization of the knowledge dissemination information type follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.20.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of knowledge dissemination information on the ability of responsible agencies to publish or broadcast information. Premature and unauthorized release of information being considered for broadcast can be harmful if the information is subsequently determined to be false or counterproductive to the knowledge dissemination mission. However, the consequences of unauthorized disclosure of most knowledge dissemination information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Unauthorized disclosure of some policies governing knowledge dissemination missions can be harmful to the agency mission (e.g., some internal Voice of America editorial policies).

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for knowledge dissemination information is ***low***.

D.20.4.2 Integrity

The consequences of unauthorized modification to or destruction of knowledge dissemination information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is normally needed. The consequences of unauthorized modification or destruction of knowledge dissemination information can generally be overcome if basic procedures and controls are implemented. In most cases, competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. Except for cases in which the integrity violation results in broadcast of erroneous information, or of information the dissemination of which is inconsistent with mission objectives or agency policy, the consequences should be limited. In cases of dissemination of erroneous/defamatory information, an agency mission can be seriously harmed and the impact of the consequences can be ***moderate***. In most cases, the consequences of unauthorized modification to or destruction of knowledge dissemination information would have, at most, a limited adverse effect on agency operations, agency assets, or individuals. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency, but the damage to the mission would usually be limited and can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for modification or destruction of most knowledge dissemination information is ***low***.

D.20.4.3 Availability

The effects of disruption of access to or use of most knowledge dissemination information or information systems would have, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: An exception might be extended disruption of broadcast capabilities (e.g., Voice of America). Here, the agency mission is seriously harmed and the impact of the consequences can be ***moderate***.

Recommended Availability Impact Level: The default availability impact level recommended for most knowledge dissemination information is ***low***.

D.21 Regulatory Compliance and Enforcement

Regulatory Compliance and Enforcement involves the direct monitoring and oversight of a specific individual, group, industry, or community participating in a regulated activity via market mechanisms, command and control features, or other means to control or govern conduct or behavior.

D.21.1 Inspections and Auditing Information Type

Inspections and Auditing involves the methodical examination and review of regulated activities to ensure compliance with standards for regulated activity. The recommended security categorization for the inspections and auditing information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, MODERATE), (**integrity**, MODERATE), (**availability**, LOW)}

D.21.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of inspections and auditing information on the ability of responsible agencies to methodically examine and review regulated activities to ensure compliance with standards for regulated activity. Note that *national security information* and *national security systems* are outside the scope of this guideline. Otherwise, where the inspections and auditing data belongs to one of the information types described in this guideline, the confidentiality impact assigned the data and system is dependent on the nature of the regulated activity. Unauthorized disclosure of inspections and auditing information can alert personnel associated with programs being monitored to the focus and implications of inspection or auditing activities. Armed with these insights, program personnel can, in some cases, divert attention from questionable program attributes, hide unfavorable information, and make cosmetic changes that fail to correct underlying deficiencies but give false impressions to inspectors and auditors. Where a major programs or human safety is at stake, actions taken based on unauthorized disclosure of inspections and auditing information can pose a threat to human life or a loss of major assets. In such cases, the confidentiality impact is ***high***.

Recommended Confidentiality Impact Level: Although there are many Federal environments in which unauthorized disclosure will have only a limited adverse effect on agency operations, assets, or individuals, there are enough circumstances in which serious adverse effects on agency operations, agency assets, or individuals can result to justify recommendation of a ***moderate*** default confidentiality impact level for inspections and auditing information.

D.21.1.2 Integrity

The consequences of unauthorized modification or destruction of inspections and auditing information can compromise the effectiveness of the program. Most back-up and archiving procedures are designed to work with copies of data as it is collected and introduced into the system. In most cases, agency personnel cannot be expected to recognize anomalous monitoring information and compare suspect information to established baselines. The damage likely to be caused by unauthorized modification or destruction of inspections and auditing information may very well adversely inspection or audit results with consequent serious adverse effects on agency operations or public confidence in the agency. The consequences can be particularly serious if the destruction or modification of information invalidates oversight of major programs or information concerning threats to human safety. Once an integrity compromise has been detected, the adverse effects can often be corrected within reasonable time and resource constraints. The integrity impact resulting from unauthorized modification or deletion of inspections and auditing information depends in part on the nature of the laws or policies with which compliance is being determined and in part on the criticality of the processes being monitored (e.g., correctness of contract expenditure reporting versus safety regulations affecting manned space flight).

Recommended Integrity Impact Level: Although there are regulatory environments in which a ***low*** impact level is appropriate, the circumstances associated with most inspections and audits support recommendation of at least a ***moderate*** default integrity impact level.

D.21.1.3 Availability

The effects of disruption of access to or use of inspections and auditing information collected to determine the effectiveness of internal and external programs and the extent to which they comply with related laws, regulations, and policies can usually be repaired within reasonable time and resource constraints. The time and resources required for recovery is largely dependent on implementation and use of mitigating procedures and controls. In most cases, disruption of access to or use of inspections and auditing information is expected to have only a limited adverse effect on agency operations, agency assets, or individuals. Not many inspection or auditing operations involve activities for which temporary loss of availability is likely to cause significant degradation in or loss of mission capability, place the agency at a significant disadvantage, result in major damage to or loss of major assets, or pose a threat to human life.

Special Factors Affecting Availability Impact Determination: Exceptions include consequences of loss of the surprise advantages inherent in unannounced inspections or audits for programs affecting human safety or critical infrastructures.

Recommended Availability Impact Level: For most inspection and audit functions, the recommended default availability impact level is ***low***.

D.21.2 Standards/Reporting Guideline Development Information Type

Standard Setting/Reporting Guideline Development involves the establishment of allowable limits associated with a regulated activity and the development of reporting requirements necessary to monitor and control compliance with allowable limits. This includes the development of requirements for product sampling and testing, emissions monitoring and control, incident reporting, financial filings, etc. The following security categorization is recommended for the standards/reporting guideline development information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.21.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of standards/reporting guideline development information on the abilities of responsible agencies to establish allowable limits associated with a regulated activity and to develop reporting requirements necessary to monitor and control compliance with allowable limits. There are some cases for which standards or guidelines include classified or other *national security information*. Such cases are outside the scope of this guideline. In a few cases, public dissemination of standards or guidelines information can harm the effectiveness of the function being supported (e.g., encouragement of tax evasion that

might result from public dissemination of Internal Revenue Service audit thresholds for certain deductions). However, most Federal standards and guidelines are, intended for public dissemination. The consequences of unauthorized disclosure of the vast majority of standards/reporting guideline development information will result in, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for standards/reporting guideline development information is ***low***.

D.21.2.2 Integrity

The consequences of unauthorized modification to or destruction of standards/reporting guideline development information depends mostly on the criticality of the information with respect to agency mission capability, protection of agency assets, and safety of individuals. Also, in the case of standards/reporting guideline development information, there is a high probability that an integrity compromise will be noticed before its consequences are felt. In any case, the effects of modifications to or deletion of this information are generally limited with respect to agency mission capabilities or assets. Any resulting damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for standards/reporting guideline development information is ***low***.

D.21.2.3 Availability

The effects of disruption of access to or use of standards/reporting guideline development information or information systems can usually be repaired within reasonable time and resource constraints. The time frame required for repair is dependent on mitigating procedures and controls. The nature of standards/reporting guideline development processes is tolerant of reasonable delays. In the case of standards/reporting guideline development records, the disruption of access to records can usually be overcome if back-up and archiving procedures are adequate and are implemented.

Recommended Availability Impact Level: The default availability impact level recommended for standards/reporting guideline development information is ***low***.

D.21.3 Permits and Licensing Information Type

Permits and Licensing involves activities associated with granting, revoking, and the overall management of the documented authority necessary to perform a regulated task or function. The following security categorization is recommended for the permits and licensing information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.21.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of permits and licensing information on the abilities of responsible agencies to manage the documented

authority necessary to perform a regulated task or function. The consequences of unauthorized disclosure of the vast majority of permits and licensing information will result in, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: Where more sensitive information is involved, it will most commonly be personal information subject to the Privacy Act of 1974, the Health Insurance Portability and Accountability Act of 1996, or other laws and executive orders affecting the dissemination of information regarding individuals. In such cases, the consequences of unauthorized disclosure of permits and licensing information could be serious, particularly in cases of exposure of data that might facilitate identity theft or support extortion (e.g., unauthorized disclosure of legal, financial, or moral misbehavior by Federal employees). In such cases, the confidentiality impact level might be ***moderate***.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for most permits and licensing information is ***low***.

D.21.3.2 Integrity

The consequences of unauthorized modification to or destruction of permits and licensing information depends mostly on the criticality of the regulated activity with respect to protection of government assets, and safety of individuals. Also, in the case of permits and licensing planning information, there is a high probability that an integrity compromise will be noticed before its consequences are felt. In any case, although there can be serious short-term effects for individuals, the effects of modifications to or deletion of this information are generally limited with respect to agency mission capabilities or assets. Any resulting damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for permits and licensing information is ***low***.

D.21.3.3 Availability

The effects of disruption of access to or use of permits and licensing information or information systems can usually be repaired within reasonable time and resource constraints. The time frame required for repair is dependent on mitigating procedures and controls. The nature of permits and licensing processes is tolerant of reasonable delays. In the case of permits and licensing records, the disruption of access to records can usually be overcome if basic procedures and controls are implemented.

Recommended Availability Impact Level: The default availability impact level recommended for permits and licensing information is ***low***.

D.22 Public Goods Creation and Management

The construction, manufacturing, administration, and/or management of goods, structures, facilities, common resources, etc. used for the general well being of the American public or society at large.

D.22.1 Manufacturing Information Type

Manufacturing involves all programs and activities in which the Federal Government produces both marketable and non-marketable goods. The following security categorization is recommended for the manufacturing information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.22.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of manufacturing information on the abilities of responsible agencies to produce both marketable and non-marketable goods. There are some cases for which manufacturing or product information includes classified or other *national security information*. Such cases are outside the scope of this guideline. In a few cases, unauthorized disclosure of details of the products or manufacturing processes can give adversaries opportunities to develop countermeasures (e.g., certain tailored law enforcement tools or instruments). However, in most cases, the consequences of unauthorized disclosure of manufacturing information will result in, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for manufacturing information is ***low***.

D.22.1.2 Integrity

The consequences of unauthorized modification to or destruction of manufacturing information depends mostly on the criticality of the information with respect to a manufacturing process and on the volume and use of the end product. In the case of most manufacturing information, there is a high probability that an integrity compromise will be noticed before its consequences are felt. In any case, the effects of modifications to or deletion of this information are generally limited with respect to agency mission capabilities or assets. Any resulting damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for manufacturing information is ***low***.

D.22.1.3 Availability

The effects of disruption of access to or use of manufacturing information or information systems can usually be repaired within reasonable time and resource constraints. The time frame required for repair is dependent on mitigating procedures and controls. The nature of most government manufacturing processes is tolerant of reasonable delays. In

the case of manufacturing records, the disruption of access to records can usually be overcome if back-up and archiving procedures are adequate and are implemented.

Recommended Availability Impact Level: The default availability impact level recommended for manufacturing information is ***low***.

D.22.2 Construction Information Type

Construction involves all programs and activities in which the Federal Government builds or constructs facilities, roads, dams, etc. The following security categorization is recommended for the construction information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.22.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of construction information on the abilities of responsible agencies to build or construct facilities, roads, dams, etc. In most cases, the consequences of unauthorized disclosure of construction information will result in, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: There are some cases for which construction includes classified or other *national security information*. Such cases are outside the scope of this guideline. In some cases, construction details can be of use to terrorists or other criminals who seek to penetrate the security of or to destroy government installations. Unauthorized disclosure to some construction details, the disclosure of which can be useful to such criminals (e.g., alarm designs, points of vulnerability to the to the structural integrity of a dam or building), can result in danger to critical infrastructures, key national assets, or human life. In such cases, the confidentiality impact can be ***high***.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for construction information is ***low***.

D.22.2.2 Integrity

The consequences of unauthorized modification to or destruction of construction information depends mostly on the criticality of the information with respect to a construction or subsequent maintenance process. In the case of most construction information, there is a high probability that an integrity compromise will be noticed before its consequences are felt. In any case, the effects of modifications to or deletion of this information are generally limited with respect to agency mission capabilities or assets. Any resulting damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for construction information is ***low***.

D.22.2.3 Availability

The effects of disruption of access to or use of construction information or information systems can usually be repaired within reasonable time and resource constraints. The time frame required for repair is dependent on mitigating procedures and controls. The nature of most government construction processes is tolerant of reasonable delays. In the case of construction records, the disruption of access to records can usually be overcome if basic procedures and controls are implemented.

Recommended Availability Impact Level: The default availability impact level recommended for construction information is ***low***.

D.22.3 Public Resources, Facilities and Infrastructure Management Information Type

Public Resources, Facilities and Infrastructure Management involves the management and maintenance of government-owned capital goods and resources (natural or otherwise) on behalf of the public, usually with benefits to the community at large as well as to the direct user. Examples of facilities and infrastructure include schools, roads, bridges, dams, harbors, and public buildings. Examples of resources include parks, cultural artifacts and art, endangered species, oil reserves, etc. The following security categorization is recommended for the public resources, facilities, and infrastructure management information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.22.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of public resources, facilities, and infrastructure management information on the abilities of responsible agencies to manage and maintain government-owned capital goods and resources (natural or otherwise) on behalf of the public, usually with benefits to the community at large as well as to the direct user. In some cases, public resources, facilities, and infrastructure management details can be of use to terrorists or other criminals who seek to penetrate the security of or to destroy government property or to harm populations. Unauthorized disclosure to some public resources, facilities, and infrastructure management details, the disclosure of which can be useful to such criminals (e.g., facilities security dispositions, building alarm designs), can result in danger to critical infrastructures, key national assets, or human life. In such cases, the confidentiality impact can be ***high***. In other cases, premature unauthorized disclosure of management information can give an unfair competitive advantage to a commercial interest (e.g., proposed changes for management of petroleum reserves). The confidentiality impact of consequent loss of public confidence and/or serious economic disruption might be ***moderate***. However, in most cases, the consequences of unauthorized disclosure of public resources, facilities, and infrastructure management information will result in, at most, a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for public resources, facilities, and infrastructure management information is ***low***.

D.22.3.2 Integrity

The consequences of unauthorized modification to or destruction of public resources, facilities, and infrastructure management information depends mostly on the criticality of the information with respect to management of public resources, facilities, and infrastructures. In the case of most public resources, facilities, and infrastructure management information, there is a high probability that an integrity compromise will be noticed before its consequences are felt. In any case, the effects of modifications to or deletion of this information are generally limited with respect to agency mission capabilities or assets. Any resulting damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The default integrity impact level recommended for public resources, facilities, and infrastructure management information is ***low***.

D.22.3.3 Availability

The effects of disruption of access to or use of public resources, facilities, and infrastructure management information or information systems can usually be repaired within reasonable time and resource constraints. The time frame required for repair is dependent on mitigating procedures and controls. The nature of most government public resources, facilities, and infrastructure management processes is tolerant of reasonable delays. In the case of public resources, facilities, and infrastructure management records, the disruption of access to records can usually be overcome if basic procedures and controls are implemented.

Recommended Availability Impact Level: The default availability impact level recommended for public resources, facilities, and infrastructure management information is ***low***.

D.22.4 Information Infrastructure Management Information Type

Information Infrastructure Management involves the management and stewardship of a type of information by the Federal Government and/or the creation of physical communication infrastructures on behalf of the public in order to facilitate communication. This includes the management of large amounts of information (e.g., environmental and weather data, criminal records, etc.), the creation of information and data standards relating to a specific type of information (patient records), and the creation and management of physical communication infrastructures (networks) on behalf of the public. Note: Information infrastructures for government use are not included here. The impact levels associated with information infrastructure maintenance information are primarily a function of the information processed in and through that infrastructure. The recommended security categorization for the information infrastructure maintenance information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.22.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of information infrastructure maintenance information on the ability of responsible agencies to manage a type of information and/or to create physical communication infrastructures on behalf of the public in order to facilitate communication. In some cases, information infrastructure maintenance details can be of use to terrorists or other criminals who seek to destroy government data bases, destroy communications infrastructures, or to deny access to information needed by the public. Unauthorized disclosure to some information infrastructure maintenance details, the disclosure of which can be useful to such criminals (e.g., passwords, authorization codes), can result in danger to critical infrastructures, key national assets, or human life. In such cases, the confidentiality impact can be ***high***. In other cases, premature unauthorized disclosure of management information can give an unfair competitive advantage to a commercial interest (e.g., proposed outsourcing of system administration or details of a proposes communications system acquisition). However, the disclosure of most information infrastructure maintenance information can be expected to result in only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The recommended default impact level recommended for information infrastructure maintenance information is ***low***.

D.22.4.2 Integrity

The consequences of unauthorized modification to or destruction of information infrastructure maintenance information usually depends on the urgency with which the information processed in and through the information infrastructure is needed or the immediacy with which the information is used. In most cases, it is unlikely that the information will be needed urgently or acted upon immediately.

Special Factors Affecting Integrity Impact Determination: In a relatively few cases the consequences of unauthorized modification of information infrastructure maintenance information that is acted upon immediately might result in more than limited damage to agency operations, assets, or human safety (e.g., information modification that results in unavailability of adverse aviation weather information in the terminal area during landing operations). In such cases, a ***moderate*** or ***high*** integrity impact level might be considered for unauthorized modification or destruction of information infrastructure maintenance information. The consequences of unauthorized modification to or destruction of information infrastructure maintenance information also depend on the adequacy of mitigating procedures and controls. The consequences of unauthorized modification or destruction of much information infrastructure maintenance information can generally be overcome if basic procedures and controls are implemented.

Recommended Integrity Impact Level: Subject to the caveats above, the default integrity impact level recommended for modification or destruction of information infrastructure maintenance information is ***low***.

D.22.4.3 Availability

The effects of disruption of access to or use of information infrastructure maintenance information or information systems can usually be expected to deny mission-critical information resources to all affected agencies. However, the consequences of unauthorized modification or destruction of much information infrastructure maintenance information can generally be overcome if basic mitigating procedures and controls implemented. In most such cases, infrastructure functionality can be restored in time to prevent catastrophic loss. Exceptions may include emergency response aspects of disaster management or other high load and time critical functions (e.g., some systems that support air traffic control functions). The availability impact level associated with unauthorized modification or destruction of information infrastructure maintenance information needed to respond to emergencies or critical to public safety can be ***high***. The far more common case is likely to be that disruption of access has a limited adverse effect on agency operations (including mission functions and public confidence in the agency), agency assets, or individuals.

Recommended Availability Impact Level: In general, where processes to which the information is essential are either not time-critical or not likely to have serious or severe consequences, the default availability impact level recommended for information infrastructure maintenance information is ***low***.

D.23 Federal Financial Assistance

Federal Financial Assistance is the provision of earned and unearned financial or monetary-like benefits to individuals, groups, or corporations.

D.23.1 Federal Grants (Non-State) Information Type

Federal Grants involve the disbursement of funds by the Federal Government to a non-Federal entity to help fund projects or activities. This includes the processes associated with grant administration, including the publication of funds availability notices, development of the grant application guidance, determination of grantee eligibility, coordination of the peer review/evaluation process for competitive grants, the transfer of funds, and the monitoring/oversight as appropriate. The general recommended security categorization for the federal grants information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.23.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of federal grants information on the ability of responsible agencies to disburse funds to non-Federal entities to help fund projects or activities. In a very few cases, details of programs for which grants are awarded may be classified or sensitive (e.g., research grants for classified intelligence community or weapons systems project activities). In such cases, some federal grants information might be classified (hence outside the scope of this guideline) or ***moderate*** to ***high*** impact. In a few cases, records associated with the grants may include information subject to privacy restrictions (e.g., the Privacy Act of 1974). In many cases, premature and unauthorized disclosure can affect the integrity of the grants

process, giving an unfair competitive advantage to one or more applicants. In such cases, punitive consequences of violations of law and/or loss of public confidence can have a seriously disruptive effect on an agency's operations and mission. In such cases, the confidentiality impact level would be ***moderate***. In the vast majority of cases, unauthorized disclosure of federal grants information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The confidentiality impact level recommended for federal grants information is ***low***.

D.23.1.2 Integrity

Federal grants activities are not generally time-critical. The consequences of unauthorized modification of federal grants information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. Furthermore, multiple individuals in multiple organizations are usually involved in the grants process. The information held by all independent parties is probably necessary to alter a grants decision. In most cases, the adverse effects of unauthorized modification to or destruction of federal grants information on agency mission functions or public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for federal grants information is ***low***.

D.23.1.3 Availability

The effects of disruption of access to or use of federal grants information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Federal grants processes are generally tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of federal grants information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for federal grants information is ***low***.

D.23.2 Direct Transfers to Individuals Information Type

Direct Transfers to Individuals involves the disbursement of funds from the Federal Government directly to beneficiaries (individuals or organizations) who satisfy Federal eligibility requirements with no restrictions imposed on the recipient as to how the money is spent. Direct Transfers include both earned and unearned Federal Entitlement programs such as Medicare, Social Security, unemployment benefits, etc. The general recommended security categorization for the direct transfers to individuals information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.23.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of direct transfers to individuals information on the ability of responsible agencies to disburse funds from the Federal Government directly to beneficiaries (individuals or organizations) who satisfy Federal eligibility requirements with no restrictions imposed on the recipient as to how the money is spent.

Special Factors Affecting Confidentiality Impact Determination: Many of the records associated with the disbursements may include information subject to privacy restrictions (e.g., the Privacy Act of 1974, HIPPA of 1996). In such cases, punitive consequences of violations of law and/or loss of public confidence can have a seriously disruptive effect on an agency's operations and mission. The consequent confidentiality impact level could be ***moderate***.

Recommended Confidentiality Impact Level: In the vast majority of cases, unauthorized disclosure of direct transfers to individuals will have only a limited adverse effect on agency operations, assets, or individuals. Therefore, the default confidentiality impact level recommended for direct transfers to individuals is ***low***.

D.23.2.2 Integrity

Federal disbursement activities are not generally time-critical (on a scale of hours or days). The consequences of unauthorized modification of direct transfers to individuals can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source material, back-up files, and/or archives. In most cases, the monetary amounts involved are not large (on a governmental budgetary scale), and adverse effects of unauthorized modification to or destruction of direct transfers to individuals on agency mission functions or public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for direct transfers to individuals is ***low***.

D.23.2.3 Availability

The effects of disruption of access to or use of information regarding direct transfers to individuals can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Federal disbursement processes are generally tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious or catastrophic damage to mission capability. The impact may be largely dependent on the scale of the disruption. Disruption of disbursements to large populations can both do serious harm to public confidence in the agency and have a harmful impact on the nation's economy (e.g., affect consumer confidents and retail sales for a month or quarter). In such cases, the availability impact would be ***moderate***. In most cases, disruption of access to or use of

information regarding direct transfers to individuals can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for direct transfers to individuals is ***low***.

D.23.3 Subsidies Information Type

Subsidies involve Federal Government financial transfers that reduce costs and/or increase revenues of producers. Subsidies include the payment of funds from the government to affect the production or prices of various goods to benefit the public. The general recommended security categorization for the subsidies information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

D.23.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of subsidies information on the ability of responsible agencies to pay government funds to affect the production or prices of various goods to benefit the public benefit. In many cases, unauthorized disclosure of subsidies information will have only a limited adverse effect on agency operations, assets, or individuals. In such cases, the confidentiality impact can be ***low***. Some information associated with applications for subsidies includes information covered by the provisions of the Privacy Act of 1974. Unauthorized disclosure of large volumes of information protected under the Privacy Act can be expected to have a serious effect on public confidence in the agency. Also, premature unauthorized disclosure of planned subsidies policies can affect financial/commodities markets, with attendant potential adverse effects on the U.S. economy and certain serious adverse effects on public confidence in the agency. Actions taken that are intended to establish blame, compensate victims or repair damage done with the exposed information can cause serious disruption of an agency's mission capability.

Recommended Confidentiality Impact Level: default confidentiality impact level recommended for subsidies information is ***low***.

D.23.3.2 Integrity

Subsidies activities are not generally time-critical. The consequences of unauthorized modification of subsidies information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In most cases, the adverse effects of unauthorized modification to or destruction of subsidies information on agency mission functions, image or public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for subsidies information is ***low***.

D.23.3.3 Availability

The effects of disruption of access to or use of subsidies information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Subsidies processes are generally tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of subsidies information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for subsidies information is ***low***.

D.23.4 Tax Credits Information Type

Tax Credits allow a special exclusion, exemption, or deduction from gross income or which provide a special credit, a preferential rate of tax, or a deferral of tax liability designed to encourage certain kinds of activities or to aid taxpayers in special circumstances. The general recommended security categorization for the tax credits information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, MODERATE), (**availability**, LOW)}

D.23.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of tax credit information on the ability of responsible agencies to allow special exclusions, exemptions, or deductions from gross income or which provide special credits, a preferential rate of tax, or a deferral of tax liability designed to encourage certain kinds of activities or to aid taxpayers in special circumstances. Many of the records associated with the disbursements may include information subject to privacy restrictions (e.g., the Privacy Act of 1974, the Internal Revenue Code and Manual, or the Economic Espionage Act). In such cases, punitive consequences of violations of law and/or loss of public confidence can have a seriously disruptive effect on an agency's operations and mission. In many cases, unauthorized disclosure of tax credit information can have a serious adverse effect on agency operations, assets, or individuals.

Recommended Availability Impact Level: The confidentiality impact level recommended for tax credit information is ***moderate***.

D.23.4.2 Integrity

Tax credits are not generally time-critical (on a scale of hours or days). The consequences of unauthorized modification of tax credits can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In most cases, the adverse effects of unauthorized modification to or destruction of tax credits on agency mission functions or public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact recommended for tax credits is ***low***.

D.23.4.3 Availability

The effects of disruption of access to or use of tax credit information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Taxation processes are generally tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of tax credit information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for tax credit information is ***low***.

D.24 Credit and Insurance

Credit and Insurance involves the use of government funds to cover the subsidy cost of a direct loan or loan guarantee or to protect/indemnify members of the public from financial losses.

D.24.1 Direct Loans Information Type

Direct loans involve a disbursement of funds by the Government to a non-Federal borrower under a contract that requires the repayment of such funds with or without interest. The general recommended security categorization for the direct loan information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.24.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of direct loan information on the ability of responsible agencies to disburse Federal funds to non-Federal borrowers under contract terms that require the repayment of such funds with or without interest. Much direct loan information includes information covered by the provisions of the Privacy Act of 1974. Unauthorized disclosure of large volumes of information protected under the Privacy Act can be expected to have a serious to severe effect on public confidence in the agency. Actions taken that are intended to establish blame, compensate victims, or repair damage done with the exposed information can cause serious disruption of an agency's mission capability. In such cases, the confidentiality impact can be ***moderate***. However, in most cases, unauthorized disclosure of direct loan information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for direct loan information is ***low***.

D.24.1.2 Integrity

Loan assistance activities are not generally time-critical. The consequences of unauthorized modification of direct loan information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In most cases, the adverse effects of unauthorized modification to or destruction of direct loan information on agency mission functions and public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact level recommended for direct loan information is ***low***.

D.24.1.3 Availability

The effects of disruption of access to or use of direct loan information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Loan assistance processes are generally tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of direct loan information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for direct loan information is ***low***.

D.24.2 Loan Guarantees Information Type

Loan guarantees involve any guarantee, insurance, or other pledge with respect to the payment of all or a part of the principal or interest on any debt obligation of a non-Federal borrower to a non-Federal lender, but does not include the insurance of deposits, shares, or other withdrawable accounts in financial institutions. The general recommended security categorization for the loan guarantees information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.24.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of loan guarantee information on the ability of responsible agencies to execute guarantees, insurance, or other pledges with respect to the payment of all or a part of the principal or interest on any debt obligation of a non-Federal borrower to a non-Federal lender. Much loan guarantee information includes information covered by the provisions of the Privacy Act of 1974. Unauthorized disclosure of large volumes of information protected under the Privacy Act can be expected to have a serious to severe effect on public confidence in the agency. In such cases, the confidentiality impact can be ***moderate***. However, in most cases, unauthorized disclosure of loan guarantee information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for loan guarantee information is ***low***.

D.24.2.2 Integrity

Loan guarantee activities are not generally time-critical. The consequences of unauthorized modification of loan guarantee information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In most cases, the adverse effects of unauthorized modification to or destruction of loan guarantee information on agency mission functions and public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact level recommended for loan guarantee information is ***low***.

D.24.2.3 Availability

The effects of disruption of access to or use of loan guarantee information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Loan processes are generally tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of loan guarantee information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Availability Impact Determination: The default availability impact level recommended for loan guarantee information is ***low***.

D.24.3 General Insurance Information Type

General Insurance involves providing protection to individuals or entities against specified risks. The specified protection generally involves risks that private sector entities are unable or unwilling to assume or subsidize and where the provision of insurance is necessary to achieve social objectives. The following security categorization is recommended for the general insurance information type:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.24.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of general insurance information on the abilities of responsible agencies to provide protection to individuals or entities against specified risks. General insurance activities include both insurance issuing and insurance servicing. Insurance issuing is any activity required of the provision of insurance such as provider approval, underwriting, and endorsements. It includes activities such as provider approval, underwriting, and endorsements. The

consequences of unauthorized disclosure of insurance issuing information will generally result in a limited adverse effect on agency operations, agency assets, or individuals.

Special Factors Affecting Confidentiality Impact Determination: The more serious consequences will often stem 1) from unauthorized disclosure of provider's (or prospective providers') proprietary information, or 2) from premature disclosure of agency plans or changes under consideration for contracts, plans, or policies. Unauthorized disclosure of information that can affect contract arrangements to the detriment of the interests of the government, and of the public at large (e.g., planned or anticipated termination of a major contract insurer), can result in damaging increases in public expense and exposure to impact. In the case of unauthorized disclosure to an individual private sector organization, unfair competitive advantage may result – with major financial consequences. In the case of unauthorized disclosure of preliminary and unsubstantiated data that is actually both incorrect and strongly pessimistic (e.g., Medicare budget projections, terrorism impact insurance shortfall projections, or anticipated failure of a major contract insurer), the consequent unwarranted alarm of the public may have serious political and operational consequences for affected agencies. In the more serious cases, the confidentiality impact incurred can be at least ***moderate***. Insurance servicing supports activities associated with administering and processing insurance. These activities include payment processing, initial and final closings, loss mitigation, claims management, and retiring insurance. The confidentiality impact level is the effect of unauthorized disclosure of insurance servicing information on the abilities of responsible agencies to administer and process insurance. These activities include payment processing, initial and final closings, loss mitigation, claims management, and retiring insurance. The consequences of unauthorized disclosure of insurance servicing information will generally result in a limited adverse effect on agency operations, agency assets, or individuals. The more serious consequences will often stem from unauthorized disclosure of private information concerning the insured (e.g., Privacy Act information).

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for general insurance information is ***low***.

D.24.3.2 Integrity

The consequences of unauthorized modification to or destruction of general insurance information depends, not only on mitigating procedures and controls, but also on the urgency with which the information is normally needed. The consequences of unauthorized modification or destruction of general insurance information can usually be overcome if basic procedures and controls are implemented. In many cases, competent agency personnel should be able to recognize anomalous information (e.g., by comparing suspect information to that contained in source materials). Where the consequences involve erroneous or fraudulent payments, eventual successful corrective action can be anticipated. Where the results take the form of delays in or denial of service, there can be more serious consequences to both the insured and to public confidence in the agency. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may have an adverse effect on agency

operations and/or public confidence in the agency. Damage can generally be corrected within reasonable time and resource constraints.

Recommended Integrity Impact Level: The integrity impact level recommended for general insurance information is ***low***.

D.24.3.3 Availability

The effects of disruption of access to or use of general insurance information or information systems can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Extensive delays in insurance servicing activities can result, not only in financial harm (or ruin) for individuals and businesses, but potentially in public alarm and repercussions in the financial markets. In the more dramatic cases, delays may have serious political and operational consequences for affected agencies. In such cases, the confidentiality impact incurred can be at least ***moderate***. The nature of general insurance processes is usually tolerant of reasonable delays. Use of basic procedures and controls (e.g., alternate communications media, back up processing facilities, and retention of copies of source material) can generally prevent major compromise of mission capability.

Recommended Availability Impact Level: Except where destruction of major facilities requires long periods of time for recovery, the default availability impact level recommended for general insurance information is normally ***low***.

D.25 Transfers to State/Local Governments

Transfers to States and Local Governments involve the transfer of funds or financial assistance from the Federal government to State and Local governments and Indian tribes.

D.25.1 Formula Grants Information Type

Formula Grants involves the allocation of money to States or their subdivisions in accordance with distribution formulas prescribed by law or administrative regulation, for activities of a continuing nature. The general recommended security categorization for the formula grants information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.25.1.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of formula grants information on the ability of responsible agencies to allocate money to States or their subdivisions in accordance with distribution formulas prescribed by law or administrative regulation, for activities of a continuing nature. In a very few cases, details of programs for which formula grants are awarded may be classified or sensitive (e.g., some Federal/State cooperative programs intended to support Homeland Security operations and involving military and/or intelligence organizations). In such cases, some formula grants information might be classified (hence outside the scope of this guideline) or ***moderate*** to ***high*** impact. In the vast majority of cases, information associated with

formula grants is public knowledge. At worst, unauthorized disclosure of most formula grants information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for formula grants information is ***low***.

D.25.1.2 Integrity

Formula grants activities are not generally time-critical. The consequences of unauthorized modification of formula grants information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Congressional records and procedures are generally adequate for this purpose. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. Furthermore, multiple individuals in multiple organizations are usually involved in the formula grants process. The information held by all independent parties is probably necessary to alter a formula grants decision. In most cases, the adverse effects of unauthorized modification to or destruction of formula grants information on agency mission functions or public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact level recommended for formula grants information is ***low***.

D.25.1.3 Availability

The effects of disruption of access to or use of formula grants information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Formula grants processes are generally tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of formula grants information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact recommended for formula grants information is ***low***.

D.25.2 Project/Competitive Grants Information Type

Project/Competitive Grants involves the funding, for fixed or known periods, of projects. Project/Competitive grants can include fellowships, scholarships, research grants, training grants, traineeships, experimental and demonstration grants, evaluation grants, planning grants, technical assistance grants, survey grants, and construction grants. The general recommended security categorization for the project/competitive grants information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.25.2.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of project/competitive grants information on the ability of responsible agencies to award fellowships, scholarships, research grants, training grants, traineeships, experimental and demonstration grants, evaluation grants, planning grants, technical assistance grants, survey grants, and/or construction grants. In a very few cases, details of programs for which grants are awarded may be classified or sensitive (e.g., research grants for classified intelligence community or weapons systems project activities). In such cases, some project/competitive grants information might be classified (hence outside the scope of this guideline) or ***moderate*** to ***high*** impact. In a few cases, records associated with the grants may include information subject to privacy restrictions (e.g., the Privacy Act of 1974). In many cases, premature and unauthorized disclosure can affect the integrity of the grants process, giving an unfair competitive advantage to one or more applicants. In such cases, punitive consequences of violations of law and/or loss of public confidence can have a seriously disruptive effect on an agency's operations and mission. In such cases, the confidentiality impact level would be ***moderate***. In the vast majority of cases, unauthorized disclosure of project/competitive grants information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for project/competitive grants information is ***low***.

D.25.2.2 Integrity

Project/competitive grants activities are not generally time-critical. The consequences of unauthorized modification of project/competitive grants information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In most cases, the adverse effects of unauthorized modification to or destruction of project/competitive grants information on agency mission functions or public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact level recommended for project/competitive grants information is ***low***.

D.25.2.3 Availability

The effects of disruption of access to or use of project/competitive grants information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Project/competitive grants processes are generally tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of project/ competitive grants information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for project/competitive grants information is ***low***.

D.25.3 Earmarked Grants Information Type

Earmarked Grants involves the distribution of money to State and Local Governments for a named purpose or service usually specifically noted by Congress in appropriations language, or other program authorizing language. The general recommended security categorization for the earmarked grants information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.25.3.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of earmarked grants information on the ability of responsible Federal government entities to distribute money to State and Local Governments for a named purpose or service usually specifically noted by Congress in appropriations language, or other program authorizing language.

Special Factors Affecting Confidentiality Impact Determination: In a very few cases, details of programs for which earmarked grants are awarded may be classified or sensitive (e.g., some Federal/State cooperative programs intended to support Homeland Security operations and involving military and/or intelligence organizations). In such cases, some earmarked grants information might be classified (hence outside the scope of this guideline) or ***moderate*** to ***high*** impact. In the vast majority of cases, earmarked grants information is public knowledge. At worst, unauthorized disclosure of most earmarked grants information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for earmarked grants information is ***low***.

D.25.3.2 Integrity

Earmarked grants activities are not generally time-critical. The consequences of unauthorized modification of earmarked grants information can generally be overcome if review procedures are in place and basic mitigating procedures and controls. Congressional records are generally adequate for comparison purposes. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. Furthermore, multiple individuals in multiple organizations are usually involved in the earmarked grants process. The information held by all independent parties is probably necessary to alter an earmarked grants decision. In most cases, the adverse effects of unauthorized modification to or destruction of earmarked grants information on agency mission functions or public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact level recommended for earmarked grants information is ***low***.

D.25.3.3 Availability

The effects of disruption of access to or use of earmarked grants information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and controls. Earmarked grants processes are generally tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of earmarked grants information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals. The default availability impact level recommended for earmarked grants information is ***low***.

D.25.4 State Loans Information Type

State Loans involve all disbursement of funds by the Government to a State or Local Government (or Indian Tribe) entity under a contract that requires the repayment of such funds with or without interest. The general recommended security categorization for the state loan information type is as follows:

SECURITY CATEGORY = {(**confidentiality**, LOW), (**integrity**, LOW), (**availability**, LOW)}

D.25.4.1 Confidentiality

The confidentiality impact level is the effect of unauthorized disclosure of state loan information on the ability of responsible agencies to disburse Federal funds a State or Local Government (or Indian Tribe) entity under a contract that requires the repayment of such funds with or without interest. In most cases, unauthorized disclosure of state loan information will have only a limited adverse effect on agency operations, assets, or individuals.

Recommended Confidentiality Impact Level: The default confidentiality impact level recommended for state loan information is ***low***.

D.25.4.2 Integrity

Loan assistance activities are not generally time-critical. The consequences of unauthorized modification of state loan information can generally be overcome if review procedures are in place and basic mitigating procedures and controls are implemented. Competent agency personnel should be able to recognize anomalous information and compare suspect information to that contained in source materials. In most cases, the adverse effects of unauthorized modification to or destruction of state loan information on agency mission functions and public confidence in the agency can be expected to be limited.

Recommended Integrity Impact Level: The default integrity impact level recommended for state loan information is ***low***.

D.25.4.3 Availability

The effects of disruption of access to or use of state loan information can usually be repaired. The time frame required for repair is dependent on mitigating procedures and

controls. Loan assistance processes are generally tolerant of delay. Basic procedures and controls, such as availability and use of back-up files and alternate facilities, can usually prevent serious or catastrophic damage to mission capability. In most cases, disruption of access to or use of state loan information can be expected to have only a limited adverse effect on agency operations, agency assets, or individuals.

Recommended Availability Impact Level: The default availability impact level recommended for state loan information is ***low***.

[This page intentionally left blank.]

APPENDIX E: LEGISLATIVE AND EXECUTIVE SOURCES ESTABLISHING SENSITIVITY/CRITICALITY

E.1 General

Some information has been established in law, by Executive Order, or by agency regulation as requiring protection from disclosure. Those information types that are national security information are outside the scope of this guideline. Each individual responsible for security categorization of an organization's information or information system should search his own department or agency's regulations for specific information protection requirements.

Some legislatively mandated prohibitions against disclosure of information (other than national security information) are identified in Table 6. The table gives the title of the section in the United States Code in which the prohibition occurs, the citation for the prohibition, and the Department, agency, or generic information type to which the law applies. Note that the information contained in the table is intended only as an aid and will not always be current. Independent law searches by analysts will generally be necessary.

Table 6: Legal Information Disclosure Prohibitions

Access to Information; Confidentiality	22 U.S.C., Chapter 46A, Section 3144	Foreign Direct Investment in United States
Access to Records	42 U.S.C., Chapter 114, Subchapter I, Part A, Section 10806	Department of Health and Human Services/Public Health Service
Administrative Enforcement; Preliminary Matters	42 U.S.C., Chapter 45, Subchapter I, Section 3610	Housing and Urban Development
Administrative Subpoenas	18 U.S.C., Part II, Chapter 223, Section 3486(a)(6)	Law Enforcement Courts
Application of Other Laws	39 U.S.C., Part I, Chapter 4, Section 410(c)	US Postal Service
Approval of Retail Food Stores and Wholesale Food Concerns	7 U.S.C., Chapter 51, Section 2018	Department of Agriculture Food Stamps
Assessment Procedures	7 U.S.C., Chapter 80, Section 4908	Department of Agriculture
Assessments (Confidential Nature)	7 U.S.C., Chapter 58, Section 2619(c)	Department of Agriculture/ *National Potato Promotion Board*
Authorization for Disclosure and Use of Intercepted Wire, Oral, or Electronic Communications	18 U.S.C., Part I Chapter 119, Section 2517(6)	Law Enforcement

Table 6: Legal Information Disclosure Prohibitions (Cont'd)		
Blood Donor Locator Service	42 U.S.C., Chapter 7, Subchapter XI, Part A, Section 1320b-11	Social Security Administration
Books and Records	7 U.S.C., Chapter 26, Subchapter III, Section 608d	Department of Agriculture
Bureau of Transportation Statistics	49 U.S.C., Subtitle I, Chapter 1, Section 111	Bureau of Transportation Statistics/Department of Transportation
Chronic Hazard Advisory Panels	15 U.S.C., Chapter 47, Section 2077	Consumer Product Safety Commission
Civil Damages for Unauthorized Inspection or Disclosure of Returns and Return Information	26 U.S.C., Subtitle F, Chapter 76, Subchapter B, Section 7431	Treasury Department/ Internal Revenue Service
Collection of Assessments; Refunds	7 U.S.C., Chapter 77, Section 4608	Department of Agriculture/ Honey Board
Confidential Information	12 U.S.C., Chapter 6A, Subchapter I, Section 635i-3(g)(3)	Treasury Department/ Bank of the Tied Aid Credit Fund
Confidential Information	15 U.S.C., Chapter 16C, Section 796	Department of Commerce/ Federal Energy Administration
Confidential Information	19 U.S.C., Chapter 14, Section 2605(i)	Treasury Department/ Cultural Property Advisory Committee
Confidential Information	21 U.S.C., Chapter 9, Subchapter VII, Part A, Section 379	Department of Health and Human Services
Confidential Information	25 U.S.C., Chapter 29, Section 2716(a)	Department of Justice/ Department of the Interior/ Bureau of Indian Affairs/ National Indian Gaming Commission
Confidential Information	30 U.S.C., Chapter 25, Subchapter V, Section 1262(b)	Environmental Protection Agency
Confidential Information	42 U.S.C., Chapter 99, Section 9122(b)	Department of Commerce/ National Oceanic and Atmospheric Administration
Confidential Information; Circumstances Permitting Disclosure	42 U.S.C., Chapter 23, Division A, Subchapter XII, Section 2181(e)	Department of Energy/ Department of Commerce/ Patent Office

Table 6: Legal Information Disclosure Prohibitions (Cont'd)		
Confidential Information; Disclosure	42 U.S.C., Chapter 65, Section 4912(b)	Environmental Protection Agency
Confidential Information; Disclosure Prohibited	12 U.S.C., Chapter 7A, Section 1141j(c)	Treasury Department/ Farm Credit Administration
Confidential Information; Trade Secrets and Secret Processes; Information Disclosure	42 U.S.C., Chapter 6A, Subchapter XII, Part E, Section 300j-4	Environmental Protection Agency
Confidential Nature (Forms for registration and fingerprinting)	8 U.S.C., Chapter 12, Subchapter II, Part VII, Section 1304(b)	Department of Justice/ Department of State/ Department of Homeland Security
Confidential Nature of Claims	38 U.S.C., Part IV, Chapter 57, Subchapter I, Section 5701	Veterans Administration
Confidential Nature of Information Furnished Bureau	15 U.S.C., Chapter 52, Section 176a	Department of Commerce/ Bureau of Foreign and Domestic Commerce
Confidential Nature of Records (Visas)	8 U.S.C., Chapter 12, Subchapter II, Part III, Section 1202(f)	Department of State/ Department of Homeland Security
Confidential or Privileged Information in an Action Described in 28 U.S.C. Sec. 1581(c)	Title XI, Rule 71, (c)	Department of Commerce/ International Trade Commission/ Judiciary
Confidential or Privileged Material	19 U.S.C., Chapter 4, Subchapter III, Part III, Section 1516a(b)(2)(B)	Department of Homeland Security/ Treasury Department/ Customs Service
Confidential Records and Information	7 U.S.C., Chapter 6, Subchapter II, Section 136e(d)	Environmental Protection Agency
Confidential Reports and Other Additional Requirements	Title I, Section 107	Departments and Agencies/Inspectors General
Confidential Status of Application	7 U.S.C., Chapter 57, Subchapter II, Part E, Section 2426	Department of Agriculture/ Plant Variety Protection Office
Confidential Status of Applications; Publication of Patent Applications	35 U.S.C., Part II, Chapter 11, Section 122	Department of Commerce/ Patent Office
Confidentiality	17 U.S.C., Chapter 2, Subchapter I, Section 57b-2	Department of Commerce/ Federal Trade Commission

Table 6: Legal Information Disclosure Prohibitions (Cont'd)		
Confidentiality	20 U.S.C., Chapter 71, Section 9007	Department of Education
Confidentiality of Abused Person's Address	42 U.S.C., Chapter 136, Subchapter III, Part B, Subpart 1, Section 13951	US Postal Service
Confidentiality of Certain Medical Records,	38 U.S.C., Part V, Chapter 73, Subchapter III, Section 7332	Veterans Administration
Confidentiality of Financial Records	12 U.S.C., Chapter 35, Section 3403	
Confidentiality of Information	7 U.S.C., Chapter 55, Section 2276	Department of Agriculture
Confidentiality of Information	18 U.S.C., Part II, Section 3509(d)(1)	Criminal Procedure: Child Victims & Child Witnesses Rights
Confidentiality of Information	22 U.S.C., Chapter 75, Section 6744	State Department
Confidentiality of Information – Non-Availability to Public	XI U.S.C., Rule 81, (h)(3)	Judiciary
Confidentiality of Medical Quality Assurance Records: Qualified Immunity for Participants	10 U.S.C., Subtitle A, Part II, Chapter 55, Section 1102	Department of Defense
Confidentiality of Records	42 U.S.C., Chapter 6A, Subchapter III-A, Part D, Section 290dd-2	Public Health Service
Counterintelligence Access to Telephone Toll and Transactional Records	18 U.S.C., Part I, Chapter 121, Section 2709	Department of Justice/ Federal Bureau of Investigation/Communication Service Providers
Crop Insurance - Purpose; Definitions; Protection of Information; Relation to Other Laws	7 U.S.C., Chapter 36, Section 1502	Department of Agriculture
Cultural Property Advisory Committee	19 U.S.C., Chapter 14, Section 2605	Treasury Department/ Department of Homeland Security
Data Collection Authority of President	10 U.S.C., Subtitle A, Part IV, Chapter 148, Subchapter II, Section 2507	Department of Defense/ National Defense Technology and Industrial Base Council

Table 6: Legal Information Disclosure Prohibitions (Cont'd)		
Disclosure, Availability, and Use of Information	49 U.S.C., Subtitle II, Chapter 11, Subchapter II, Section 1114	National Transportation Safety Board
Disclosure of Confidential Information Generally	18 U.S.C., Part I, Chapter 93, Section 1905	
Disclosure of Data	15 U.S.C., Chapter 53, Subchapter 1, Section 2613	Environmental Protection Agency
Disclosure of Information	29 U.S.C., Chapter 22, Section 2008	Department of Labor Polygraph
Disclosure of Information by Commission	15 U.S.C., Chapter IID, Subchapter II, Section 80b-10	Securities and Exchange Commission
Disclosure of Information in Possession of Social Security Administration or Department of Health and Human Services	42 U.S.C. Chapter 7, Subchapter XI, Part A, Section 1306	Social Security Administration/Department of Health and Human Services/Public Health Service
Disclosure of Wagering Tax Information	26 U.S.C., Subtitle D, Chapter 35, Subchapter C, Section 4424	Treasury Department
Disclosures to FBI for counterintelligence purposes	15 U.S.C., Chapter 41, Subchapter III, Section 1681u	
Disclosure to Foreign Antitrust Authority of Antitrust Evidence	15 U.S.C., Chapter 88, Section 6201	Department of Justice/Federal Trade Commission
Disposition of Rights	35 U.S.C., Part II, Chapter 18, Section 202(c)(5)	Department of Commerce Patent Rights
Dissemination of Unclassified Information	42 U.S.C., Chapter 23, Division A, Subchapter XI, Section 2168	Department of Energy
Employees of Nonappropriated Fund Instrumentalities: Reprisals	10 U.S.C., Subtitle A, Part II, Chapter 81Sec. 1587(e)	Department of Defense
Equal Employment Opportunities Enforcement Provisions	42 U.S.C., Chapter 21, Subchapter 6, Section 2000e-5	Equal Employment Opportunities Commission
Evidence, Procedure, and Certification for Payments	42 U.S.C., Chapter 7, Subchapter II, Section 405	Social Security Numbers
Table 6: Legal Information Disclosure Prohibitions (Cont'd)		
Federal Parent Locator	42 U.S.C., Chapter 7,	Department of Health and

Service	Subchapter IV, Part D, Section 653(b)(2)	Human Services
Fund for Rural America	7 U.S.C., Chapter 55, Section 2204f(c)(1)(D)	Treasury Department
General Provisions	7 U.S.C., Chapter 38, Subchapter II, Part E, Section 1636	Department of Agriculture Livestock Reporting
General Provisions Governing Discovery	Title V, Depositions and Discovery, Rule 26	Courts
General Provisions Respecting Control of Devices Intended for Human Use	7 U.S.C., Chapter 9, Subchapter V, Part A, Section 360j	Department of *Health and Human Services*
General Rules Regarding Provision of Assistance	7 U.S.C., Chapter 88, Subchapter VI, Section 5906	Department of Agriculture/ Alternative Agricultural Research and Commercialization Corporation
Identifying Numbers	126 U.S.C., Subtitle F, Chapter 61 Subchapter B, Section 6109	Department of Agriculture
Information	30 U.S.C., Chapter 29, Section 1733	Department of the Interior
Information Collection	16 U.S.C., Chapter 38, Subchapter V, Section 1881a	Department of Commerce Fisheries
Inspector General for Agency	50 U.S.C., Chapter 15, Section 403q(e)(3)(A)	Central Intelligence Agency
Interagency Data Sharing	12 U.S.C., Chapter 16, Section 828b	Treasury Department
Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited	18 U.S.C., Part I, Chapter 119, Section 2511	
Inspector General	22 U.S.C., Chapter 52, Subchapter II, Section 3929	State Department
Investigations	42 U.S.C., Chapter 21, Subchapter VI, Section 2000e-8	Equal Employment Opportunity Commission
Jurisdiction	28 U.S.C., Part III, Chapter 44, Section 652(d)	Courts

Table 6: Legal Information Disclosure Prohibitions (Cont'd)

Limitations on access to	38 U.S.C., Part IV,	Department of Veterans

financial records	Chapter 53, Section 5319	Affairs
Maps, Charts, and Geodetic Data: Public Availability; Exceptions	10 U.S.C., Subtitle A, Part I, Chapter 22, Subchapter II, Section 455	Department of Defense
Miscellaneous Provisions	12 U.S.C., Chapter 7A, Section 1141j	Farm Credit Administration/Treasury Department
National Program of Cancer Registries	42 U.S.C., Chapter 6A, Subchapter II, Part M, Section 280e	Department of Health and Human Services/Public Health Service
Noncombatant Assistance to United Nations	22 U.S.C., Chapter 7, Section 287d-1(d)	State Department
Notice of Defendant's Intention to Disclose Classified Information	18 U.S.C., Unlawful Possession or Receipt of Fire Arms, Section 1201 to 1203, Interstate Agreement on Detainers, Sec. 5	Courts
Obligation to Make Royalty Payments	17 U.S.C., Chapter 10, Subchapter C, Section 1003(c)(2)	Department of Commerce
Obligations With Respect to Disclosures of Personal Information	15 U.S.C., Chapter 94, Subchapter I, Section 6802	Financial
Patents and Technical Information	22 U.S.C., Chapter 32, Subchapter III, Part I, Section 2356	
Paul D. Coverdell Drug-Free Workplace Program	15 U.S.C., Chapter 14A, Section 654	Medical Information
Payment of Cost of Testing for Sexually Transmitted Diseases	42 U.S.C., Chapter 136, Subchapter III, Part E, Section 14011	Law Enforcement
Penalties for Disclosure of Information	8 U.S.C., Chapter 12, Subchapter II, Part IX, Section 1367	Department of Justice
Permissive Provisions	7 U.S.C., Chapter 79, Section 4810	Department of Agriculture
Permissive Terms and Conditions in Orders	7 U.S.C., Chapter 60, Section 2706	Department of Agriculture/ Egg Board
Petroleum Product Information	33 U.S.C., Chapter 12, Subchapter I, Section 555a(d)	Army Corps of Engineers/ Department of Defense

Table 6: Legal Information Disclosure Prohibitions (Cont'd)

Physical Protection of	10 U.S.C., Subtitle A, Part	Department of Energy

Special Nuclear Material: Limitation on Dissemination of Unclassified Information	I, Chapter 3, Section 128	
Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records	18 U.S.C., Part I, Chapter 123, Section 2721	States
Program Requirements	42 U.S.C., Chapter 13, Section 1758	Department of Agriculture/ Public Health Service
Prohibition Against Disclosure of Information	42 U.S.C., Chapter 7, Subchapter XI, Part B, Section 1320c-9	Department of Health and Human Services/ Public Health Service/ Social Security Administration
Prohibition of Advance Disclosure of Funding Decisions	42 U.S.C., Chapter 44, Section 3537a	Department of Housing and Urban Development
Prohibition Against Disclosure of Information or Knowledge	22 U.S.C., Chapter 7, Section 287t	International Monetary Fund
Prohibition of Public Disclosure of Proprietary Information	12 U.S.C., Chapter 46, Section 4546	Treasury Department
Protection of Trade Secrets and Other Information	7 U.S.C., Chapter 6, Subchapter II, Section 136h	Department of Agriculture/ Environmental Protection Agency
Provision of Certain Counseling Services	42 U.S.C., Chapter 6A, Subchapter XXIV, Section 300ff-62	Department of Health and Human Services/Public Health Service
Provisions	22 U.S.C., Chapter 58, Subchapter III, Section 4833	State Department
Provisions Relating to Disclosures of Violations of Law, Gross Mismanagement, and Certain Other Matters	5 U.S.C., Part II, Chapter 12, Subchapter II, Section 1213(h)	Office of Personnel Management
Public Access to Information	33 U.S.C., Chapter 29, Section 1513	Department of Transportation/ Department of Homeland Security
Public Disclosure	7 U.S.C., Chapter 7, Section 12	Commodity Futures Trading Commission

Table 6: Legal Information Disclosure Prohibitions (Cont'd)

Public Disclosure of Final	12 U.S.C., Chapter 46,	Treasury Department

Orders and Agreements (Government Sponsored Enterprises)	Sections 4522, 4586 and 4639	
Public Disclosure of Information	15 U.S.C., Chapter 47, Section 2055	Consumer Product Safety Commission
Recommendations by Promotion Boards	10 U.S.C., Subtitle E, Part III, Chapter 1403, Section 14108	Department of Defense
Recordkeeping, Inspections, Monitoring, and Entry	42 U.S.C., Chapter 85, Subchapter I, Part A, Section 7414(c)	Environmental Protection Agency
Records and Reports; Inspections	33 U.S.C., Chapter 26, Subchapter III, Section 1318	Water Pollution
Records Maintained on Individuals	5 U.S.C., Part I, Chapter 5, Subchapter II, Section 552a	Privacy Act
Reporting Requirements; Disclosure of Information	16 U.S.C., Chapter 16C, Section 973j	Department of Commerce
Reports of Information Regarding Safety and Soundness of Depository Institutions	12 U.S.C., Chapter 16, Section 1831m-1(a)(2)(B)	Financial
Reports; Recordkeeping; Investigations	29 U.S.C., Chapter 30, Subchapter V, Section 2935(a)(4)(B)(i)	Department of Labor
Requests by Authorized Investigative Agencies	50 U.S.C., Chapter 15, Section 436	Intelligence Community
Required Terms in Orders	7 U.S.C., Chapter 101, Subchapter V, Section 7484	Department of Agriculture/ Popcorn Board
Required Terms of Order; Agreements Under Order; Records	7 U.S.C., Chapter 76, Subchapter II, Section 4534	Department of Agriculture/ National Dairy Research Endowment Institute
Research on Transplantation of Fetal Tissue	42 U.S.C., Chapter 6A, Subchapter III, Part H, Section 289g-1(d)(2)	Department of Health and Human Services/National Institutes of Health
Restriction of Access by Minors to Materials Commercially Distributed by Means of World Wide Web that are Harmful to Minors	47 U.S.C., Chapter 5, Subchapter II, Part I, Section 231	
Table 6: Legal Information Disclosure Prohibitions (Cont'd)		
Restrictions on Disclosing and Obtaining Contractor	41 U.S.C., Chapter 7, Section 423	

Bid or Proposal Information or Source Selection Information		
Right to Financial Privacy	12 U.S.C., Chapter 35	
Rights in Technical	10 U.S.C., Subtitle A, Part IV, Chapter 137, Section 2313, Sec. 2320	Department of Defense
Rules and Regulations	22 U.S.C., Chapter 46, Section 3104(c)	State Department
Safeguards Information,	42 U.S.C, Chapter 23, Division A, Subchapter XI, Section 2167	Department of Energy
Safety Performance History of New Drivers; Limitation on Liability	49 U.S.C., Subtitle I, Chapter 5, Subchapter I, Section 508(b)	Motor Carrier
Security and Research and Development Activities	49 U.S.C., Subtitle VII, Part A, Subpart i, Chapter 401, Section 40119(b)(1)	Federal Aviation Administration
Special Provisions Concerning the Department of Justice	5 U.S.C., Federal Advisory Committee Act, Section 8E	Department of Justice
Special Provisions Concerning the Department of the Treasury	5 U.S.C., Federal Advisory Committee Act, Section 8D	Treasury Department
Submission of Purchase Intentions by Cigarette Manufacturers	7 U.S.C., Chapter 35, General Provisions, Section 1314g	Department of Agriculture
Transition Period	45 U.S.C., Chapter 21, Section 1204	Department of Transportation Railroads
Unauthorized Disclosure of Information	26 U.S.C., Subtitle F, Chapter 75, Subchapter A, Part I, Section 7213	Treasury Department/IRS
Unlawful Disclosure of Information	49 U.S.C., Subtitle IV, Part C, Chapter 161, Section 16103	Department of Transportation Pipeline Carriers
Unlawful Possession or Receipt of Firearms, Federal Rules of Criminal Procedure, The Grand Jury	18 U.S.C., Sections 1201-1203, Sec. 16, I, Rule 6	Courts
Verification of Compliance	22 U.S.C., Chapter 35, Subchapter III, Section 2577d	State Department
Table 6: Legal Information Disclosure Prohibitions (Cont'd)		
Voluntary Disclosure of Customer Communications	18 U.S.C., Part I, Chapter121, Section 2702	

or Records		
Written Evaluations	12 U.S.C., Chapter 30, Section 2906	Treasury Department/ Comptroller of the Currency/ Federal Reserve System/ Federal Deposit Insurance Corporation/
Wrongful Disclosure of Information	13 U.S.C., Chapter 7, Subchapter I, Section 214	Census Bureau Census Information
Wrongful Disclosure of Video Tape Rental or Sale Records	18 U.S.C., Part 1, Chapter 121, Section 2710	

E.2 OMB and Case Law Interpretations

The disclosure prohibitions, as stated in law are often imprecise. As a result, Office of Management and Budget and case law interpretations are sometimes necessary to clarify the prohibitions. In some cases, the analyst may need to identify such clarifications and interpretations.

One law imposing disclosure prohibitions that has received particular attention across the Federal government deserves special attention. The Privacy Act of 1974, 5 U.S.C. § 552a (2000), which has been in effect since September 27, 1975, can generally be characterized as an omnibus "code of fair information practices" that attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal executive branch agencies. However, the Act's imprecise language, limited legislative history, and somewhat outdated regulatory guidelines have rendered it a difficult statute to decipher and apply. Moreover, even after more than twenty-five years of administrative and judicial analysis, numerous Privacy Act issues remain unresolved or unexplored. Adding to these interpretational difficulties is the fact that many Privacy Act cases are unpublished district court decisions.

A primary element of the Privacy Act of 1974 is the “no disclosure without consent” rule: *No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains [subject to 12 exceptions]." 5 U.S.C. § 552a(b).*

Note that a "disclosure" can be by any means of communication - written, oral, electronic, or mechanical. [See OMB Guidelines, 40 Fed. Reg. 28,948, 28,953 (1975).] Details of the Privacy Act of 1974, together with OMB and judicial interpretations can be found on the Department of Justice web site, http://www.usdoj.gov/04foia/04_7_1.html.

Subsection (v) of the Privacy Act requires the Office of Management and Budget (OMB) to: (1) "prescribe guidelines and regulations for the use of agencies in implementing" the Act; and (2) "provide continuing assistance to and oversight of the implementation" of the Act by agencies. 5 U.S.C. § 552a(v). The vast majority of OMB's Privacy Act

Guidelines (OMB Guidelines) are published at 40 Fed. Reg. 28,948-78 (1975). However, these original guidelines have been supplemented in particular subject areas over the years. 40 Fed. Reg. 56,741-43 (1975) (system of records definition, routine use and intra-agency disclosures, consent and congressional inquiries, accounting of disclosures, amendment appeals, rights of parents and legal guardians, relationship to Freedom of Information Act (FOIA)); 48 Fed. Reg. 15,556-60 (1983) (relationship to Debt Collection Act); 52 Fed. Reg. 12,990-93 (1987) ("call detail" programs); 54 Fed. Reg. 25818-29 (1989) (computer matching); 56 Fed. Reg. 18,599-601 (proposed Apr. 23, 1991) (computer matching); 61 Fed. Reg. 6428, 6435-39 (1996) ("Federal Agency Responsibilities for Maintaining Records About Individuals").

As a general rule, the OMB Guidelines are entitled to the deference usually accorded the interpretations of the agency that has been charged with the administration of a statute. Quinn v. Stone, 978 F.2d 126, 133 (3d Cir. 1992); Baker v. Dep't of the Navy, 814 F.2d 1381, 1383 (9th Cir. 1987); Perry v. FBI, 759 F.2d 1271, 1276 n.7 (7th Cir. 1985) (citing Bartel v. FAA, 725 F.2d 1403, 1408 n.9 (D.C. Cir. 1984); Albright v. United States, 631 F.2d 915, 919 n.5 (D.C. Cir. 1980)), rev'd en banc on other grounds, 781 F.2d 1294 (7th Cir. 1986); Smiertka v. United States Dep't of the Treasury, 604 F.2d 698, 703 n.12 (D.C. Cir. 1979); Rogers v. United States Dep't of Labor, 607 F. Supp. 697, 700 n.2 (N.D. Cal. 1985); Sanchez v. United States, 3 Gov't Disclosure Serv. (P-H) ¶ 83,116, at 83,709 (S.D. Tex. Sept. 10, 1982); Golliher v. United States Postal Serv., 3 Gov't Disclosure Serv. (P-H) ¶ 83,114, at 83,703 (N.D. Ohio June 10, 1982); Greene v. VA, No. C-76-461-S, slip op. at 6-7 (M.D.N.C. July 3, 1978); Daniels v. FCC, No. 77-5011, slip op. at 8-9 (D.S.D. Mar. 15, 1978); see also Martin v. Office of Special Counsel, 819 F.2d 1181, 1188 (D.C. Cir. 1987) (OMB interpretation is "worthy of our attention and solicitude"). However, a few courts have rejected particular aspects of the OMB Guidelines as inconsistent with the statute. Kassel v. VA, No. 87-217-S, slip op. at 24-25 (D.N.H. Mar. 30, 1992) (subsection (e)(3)); Saunders v. Schweiker, 508 F. Supp. 305, 309 (W.D.N.Y. 1981) (same); Metadure Corp. v. United States, 490 F. Supp. 1368, 1373-74 (S.D.N.Y. 1980) (subsection (a)(2)); Fla. Med. Ass'n v. HEW, 479 F. Supp. 1291, 1307-11 (M.D. Fla. 1979) (same); Zeller v. United States, 467 F. Supp. 487, 497-99 (E.D.N.Y. 1979) (same).