NIST Special Publication 800-60
Version 1.0
Initial Public Draft

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

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

William C. Barker

INFORMATION SECURITY

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 I, 38 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 authors 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

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.

This is Volume I of two volumes. It contains the basic guidelines for mapping types of information and information systems to security categories. The appendices, including security categorization recommendations for agency-specific information types and rationale for security categorization recommendations, are published as a separate volume.

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.

[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.

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.

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

Table of Contents

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

Guide for Mapping Types of Information and Information Systems To Security Categories

1.0 INTRODUCTION

Title III of the E-Government Act (Public Law 107-347), titled the Federal Information Security Management Act (FISMA), tasked 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 category; and
- Minimum information security requirements (i.e., management, operational, and technical controls), for information and information systems in each such category.

The purpose of NIST Special Publication 800-60 is to address the second FISMA-related task— development of guidelines recommending the types of information and information systems to be included in each category of potential security impact. This will help agencies to map security impact levels, in a consistent manner to types of: (i) information (e.g., privacy information, medical information, proprietary information, financial information, contractor sensitive information, trade secret information, investigation information); and (ii) information systems (e.g., mission critical systems, mission support systems, administrative systems).

Types of information can normally be divided into information associated with an agency's mission-specific activities and 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 the consequences of security compromise of mission-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 identified in the guideline, 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 provided in Appendix D).

1.1 Structure

This guideline is divided into two volumes. Volume I provides information type identification and security categorization guidelines. Volume II consists of the appendices, including examples of security categorization rationale.

Volume I provides the following background information and mapping guidelines:

- Section 2: An overview of the security objectives and impact levels identified in the Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems* [FIPS 199],
- Section 3: Overview of the process used to select impact levels, general considerations relating to impact assignment, and guidelines for system categorization,
- Section 4: Guidelines for identification of mission information types and for assignment of security impact levels to mission information, and
- Section 5: Recommended default security impact levels by type for administrative, management, and service information.

Volume II includes the following appendices:

- Appendix A: Glossary,
- Appendix B: References,
- Appendix C: Rationale for assignment of default security impact levels by type for administrative, management, and service information,
- Appendix D: Sample mission information and services delivery mechanism impact assignments, and
- Appendix E: Legislative and executive sources that specify sensitivity/criticality properties.

This guideline is intended as a reference resource rather than as a tutorial. Not all of the material will be relevant to all agencies. It is intended that users will review the introductory material, terminology, and process material in the first three sections of the guideline. The users should review the guidelines for assignment of impact levels found in Section 4 for mission information and Section 5 for administrative, management, and service information. The user then needs to refer to only that material from the rest of the guideline that applies to his or her systems and applications. Material intended to support review of default impact levels is included in Appendices C, D, and E.

1.2 Applicability

This recommendation applies to all Federal systems other than *national security systems*. *National security systems* store, process, or communicate *national security* information.[2]

[2] FISMA defines a *national security system* as 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;

2.0 SECURITY CATEGORIZATION OF INFORMATION AND INFORMATION SYSTEMS

Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199), defines the security categories, security objectives, and impact levels to which this guide maps information types. FIPS 199 also describes the context of use for this guideline. Some of the content of FIPS 199 is included in this section in order to simplify the use of this guideline.

Most Federal government agencies do have both the expertise and information base to determine the potential impact level or magnitude of harm that can be expected to result from a loss of confidentiality, integrity, and availability of their information and/or information systems. FIPS 199 establishes security categories based on the magnitude of harm that can be expected to result from compromises rather than on the results of an assessment that includes an attempt to determine the probability of compromise.

This SP 800-60 guideline recommends default impact levels for specific information types. It also provides some rationale for these recommended default levels and discusses some of the circumstances that might result in assignment of impact levels higher or lower than the recommended default levels. The guideline stresses that the impact level associated with agency-common information is strongly affected by the agency-specific information with which it is associated. Each organization should review the recommended information impact levels in the context of its own operational environment, then accept or revise impact levels accordingly. The impact level of information can be defined only within the context of an organization's operational environment. The same information types that may have low impact in the operational context of one organization or operation may have a high impact level in another organizational or operational context.

Generally, information systems process many types of information. Not all of these information types are likely to have the same impact levels. The compromise of some information types will jeopardize system functionality and agency mission more than the compromise of other information types. System impact levels must be assessed in the context of system mission and function as well as on the basis of the aggregate of the component information types.

---

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.

2.1 Security Categories and Objectives (Contents from FIPS 199)

2.1.1 Security Categories

FIPS 199 establishes security categories for both information[3] and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

FIPS Pub 199 establishes three potential levels of impact (low, moderate, and high) relevant to securing Federal information and information systems for each of three stated security objectives (confidentiality, integrity, and availability).

2.1.2 Security Objectives and Types of Potential Losses

FISMA and FIPS 199 define three security objectives for information and information systems.

2.1.2.1 Confidentiality

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

A loss of *confidentiality* is the unauthorized disclosure of information.

2.1.2.2 Integrity

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

A loss of *integrity* is the unauthorized modification or destruction of information.

2.1.2.3 Availability

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of *availability* is the disruption of access to or use of information or an information system.

2.2 Impact Assessment (Contents from FIPS 199)

The application of the FIPS 199 definitions for levels of *potential impact* on organizations or individuals should there be a breach of security must take place within the context of each organization and the overall national interest.

[3] Information is categorized according to its *information type*. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management), defined by an organization, or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

2.2.1 Levels of Impact

The potential impact is **low** if—

- The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. [4]

  A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

The potential impact is **moderate** if—

- The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

  A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is **high** if—

- The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

  A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

2.2.2 Establishment of Security Categories for Information Types

In FIPS 199, the security category of an information type can be associated with both user information and system information[5] and can be applicable to information in either

[4] Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

electronic or non-electronic form. It is also used as input in considering the appropriate security category for a system. Establishing an appropriate security category for an information type simply requires determining the *potential impact* for each security objective associated with the particular information type. The generalized format for expressing the security category, or *SC*, of an information type is:

SECURITY CATEGORY $_{\text{information type}}$ = {[(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}

where the acceptable values for potential *impact* are low, moderate, high, or not applicable. [6]

[5] System information (e.g., network routing tables, password files, and cryptographic key management information), must be protected at a level commensurate with the most critical or sensitive user information being processed by the information system to ensure confidentiality, integrity, and availability.

[6] The potential impact value of *not applicable* may be applied only to the confidentiality security objective.

3.0 ASSIGNMENT OF IMPACT LEVELS AND SECURITY CATEGORIZATION

3.1 Mapping Information Types to Security Objectives and Impact Levels

This subsection provides a step-by-step methodology for mapping information types and information systems to security objectives and impact levels. Assignment of security levels is based on FIPS 199. This document assumes that the user has read and is familiar with FIPS 199.

Figure 1 illustrates the security categorization process and how security categorization fits into the process of selecting security controls. This process is performed for every information system.

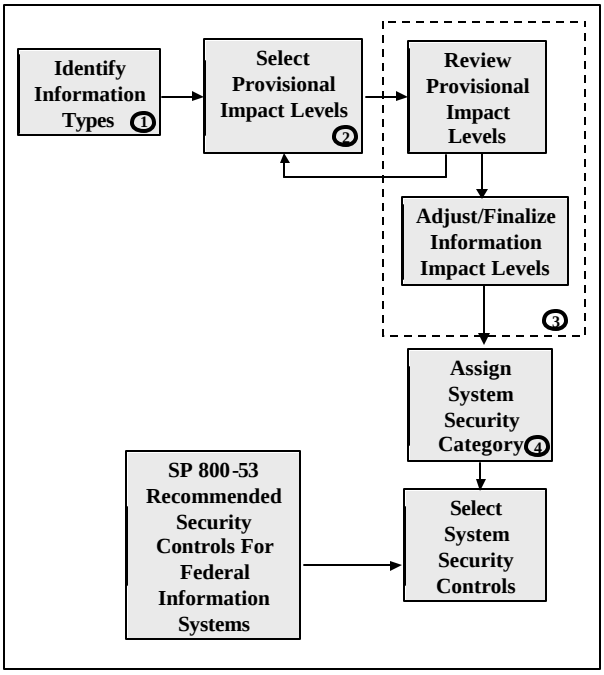

Figure 1: FIPS 800-60 Security Categorization Process

1. Identify information types. The user should first identify all of the information types that are input into, stored in, processed by, and/or output from the system.

2. Select provisional impact levels. The user should then provisionally assign impact levels to each identified information type.

3. Review provisional impact levels. Next, the user should review the appropriateness of the default impact levels recommended for the user's

information types in the context of the organization, environment, mission, use, and connectivity associated with the system under review.

4. Adjust/finalize information impact levels. Based on the results of the review of provisional impact levels, adjustments should be made to the recommended default impact levels as appropriate.

5. Assign system security category. The user now establishes the level of confidentiality impact, integrity impact, and availability impact associated with the system under review. The adjusted impact levels for information types are reviewed with respect to the aggregate of all information processed in or by each system. In some cases, the consequences of loss of confidentiality, integrity, or availability of the information aggregate can be more serious than that for any single information type. In addition, a system's access control information and the system software that protects and invokes it can both affect the integrity and availability attributes of a system and even access to other systems to which the system under review is connected.

Following completion of the security categorization process, the confidentiality, integrity, and availability impact level determinations that result from this process can then be used to select the set of security controls necessary for each system. The minimum security controls recommended for each system security category can be found in NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems.*

3.2 Information Type Identification

A methodology that can be employed for identification of information types is to:

- Identify the fundamental business areas or mission areas supported by the system under review;

- For each business area or mission area, identify internal and/or external operations areas or lines of business that describe the purpose of the system in functional terms;

- Identify the sub-functions necessary to carry out each area of operations or line of business;

- Identify basic information types with the identified sub-functions; and where appropriate,

- Identify any information type processed by the system that is required by statute, executive order, or agency regulation to receive special handling (e.g., with respect to unauthorized disclosure or dissemination). This information may be used to adjust the information type or system impact levels.

"Business areas" separate government operations into high-level categories relating to the purpose of government, the mechanisms the government uses to achieve its purposes, the support functions necessary to conduct government operations, and resource management functions that support all areas of the government's business.

"Areas of operation" or "lines of business" describe the *purpose* of government in functional terms or describe the support functions that the government must conduct in order to effectively deliver services to citizens. *Lines of business* relating to the purpose of government and the mechanisms the government uses to achieve its purposes tend to be agency-specific. A preliminary list of these agency-specific information types is provided in Appendix D.

Lines of business relating to support functions and resource management functions that are necessary to conduct government operations tend to be common to most agencies. Agency-common lines of business that are identified in the Office of Management and Budget's Federal Enterprise Architecture Program Management Office publication, *The Business Reference Model Version 2.0* (*BRM*) are listed in Section 5 below. The definition for each of these "lines of business" is provided in Appendix C.

Sub-functions are the basic operations employed to provide the system services within each area of operations or line of business. Some examples of sub-functions that are components of agency-specific lines of business are provided in Appendix D. Agency-common sub-functions that are identified for each line of business in the *BRM* are listed in Section 5 and defined in Appendix C.

An information type is identified for each sub-function listed.

Appendix E, lists legislative and executive sources that establish sensitivity or criticality protection requirements for specific information types.

Although this guideline identifies a number of information types and bases its taxonomy on the *BRM*, only a few of the types identified are likely to be processed by any single system. Also, each system may process information that does not fall neatly into one of the listed information types. Once a set of information types identified in this guideline has been selected, it is prudent to review the information processed by each system under review to see if additional types need to be identified for impact assessment purposes.

3.3 Selection of Provisional Impact Levels

Section 5 suggests default confidentiality, integrity, and availability impact levels for agency-common information types, and Appendix D suggests default impact levels for some agency-specific information types. Where an information type processed by a system is not categorized by this guideline, an initial impact determination will need to be made based on the following FIPS 199 criteria.

3.3.1 FIPS 199 Security Categorization Criteria

An agency may identify information types not listed in this guideline or may choose not to select a default impact level from Section 5 (for agency-common information types) or Appendix D (for agency-specific information types). If this is the case, the agency should employ the following FIPS 199 criteria to determine provisional impact levels.

Agencies can assign security categories for information types and information systems by selecting and adjusting appropriate values for the potential impact of compromises of confidentiality, integrity, and availability. Table 1, "Categorization of Federal Information and Information Systems," provides the criteria for selecting impact levels for information and information systems. Those responsible for impact selection and subsequent security categorization should apply the criteria provided in Table 1 to each information type received by, processed in, stored in, and/or generated by each system for which they are responsible. The security categorization will generally be determined based on the most sensitive or critical information received by, processed in, stored in, and/or generated by the system under review.

TABLE 1: CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS

	POTENTIAL IMPACT		
SECURITY OBJECTIVE	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

3.3.2 Examples of FIPS 199-Based Selection of Impact Levels

FIPS 199-based examples of impact selection and security categorization for sample information types and systems follow:

EXAMPLE 1: An organization managing *public information* on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. The resulting security category, SC, of this information type is expressed as:

SECURITY CATEGORY $_{\text{public information}}$ = {(**confidentiality**, n/a), (**integrity**, moderate), (**availability**, moderate)}.

EXAMPLE 2: A law enforcement organization managing extremely sensitive *investigative information* determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate. The resulting security category, or *SC*, for this type of information is expressed as:

SECURITY CATEGORY$_{\text{investigative information}}$ = [(**confidentiality**, high), (**integrity**, moderate), (**availability**, high)].

EXAMPLE 3: A financial organization managing routine *administrative information* (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security category, SC, of this information type is expressed as:

SECURITY CATEGORY$_{\text{routine administrative information}}$ = [(**confidentiality**, low), (**integrity**, low), (**availability**, low)].

In general, impact assessment is independent of mechanisms employed to mitigate the consequences of a compromise.

3.3.3 Other Factors for Selection of Impact Levels

Where an agency determines impact levels and security categorization based on local application of FIPS 199 criteria, it is recommended that the following questions and factors be considered with respect to security impacts for each information type:

- ***Common Confidentiality Factors***

  Using the FIPS 199 impact criteria summarized in Table 1, each information type should be evaluated with respect to the low/moderate/high impact associated with the answers to the following questions:

+ How can a malicious adversary use the information to do limited/serious/severe harm to agency operations, agency assets, or individuals?

+ How can a malicious adversary use the information to gain control of agency assets that might result in unauthorized modification of information, destruction of information, or denial of system services that would result in limited/serious/severe harm to agency operations, agency assets, or individuals?

+ Would unauthorized disclosure/dissemination of elements the information type violate laws or executive orders or agency regulations?

Each use of the information type and each known variant of the information belonging to the type should be considered in determining the confidentiality impact level.

- ***Common Integrity Factors:***

Using the FIPS 199 impact criteria summarized in Table 1, each information type should be evaluated with respect to the low/moderate/high impact associated with unauthorized modification or destruction of 1] each known variant of the information belonging to the type and 2] each use for the information by the system under review.

Unauthorized modification or destruction of information can take many forms. The changes can be subtle and hard to detect, or they can occur on a massive scale. One can construct an extraordinarily wide range of scenarios for modification of information and its likely consequences. Just a few examples include forging information or modifying information to mislead can be accomplished in order to reduce public confidence in an agency, to fraudulently achieve financial gain, to create confusion or controversy by promulgating a fraudulent or incorrect procedure, to initiate confusion or controversy through false attribution of a fraudulent or false policy, to influence personnel decisions, to interfere with or to manipulate law enforcement or legal processes, to influence legislation, and to achieve unauthorized access to government information or facilities. In most cases, the most serious impacts of integrity compromise occur when some action is taken that either is based on the modified information or disseminates the modified information to other organizations or the public.

Undetected/unmitigated loss of integrity can be catastrophic in the case many information types. The consequences of integrity compromise can be either direct (e.g., modification of a financial entry, medical alert, or criminal record) or indirect (e.g., facilitate unauthorized access to sensitive or private information or deny access to information or information system services). Unconstrained malicious write access to information and information systems can do enormous harm to an agency's

missions and can be employed to use an agency system as a proxy for attacks on other missions.

In many cases, the consequences of unauthorized modification to or destruction of information to agency mission functions and public confidence in the agency can be expected to be limited. In other cases, integrity compromises can result endangerment of human life or other severe consequences. The impact can be particularly severe in the case of time-critical information.

- ***Common Availability Factors:***

  Using the FIPS 199 impact criteria summarized in Table 1, each information type should be evaluated with respect to the low/moderate/high impact associated with loss of availability of 1] each known variant of the information belonging to the type and 2] each use for the information by the system under review.

  For many information types and information systems, the availability impact level depends on how long the information or system remains unavailable. Undetected/unmitigated loss of availability can be catastrophic in the case many information types. For example, permanent loss of program monitoring, budget formulation, budget execution, contingency planning, continuity of operations, service recovery, debt collection, federal asset sales, taxation management, personnel management, payroll management, security management, inventory control, logistics management, budget and finance, or accounting information data bases would be catastrophic for almost any agency. Complete reconstruction of such databases would be time-consuming and expensive. The disruption to agency operations would be serious to severe.

  In most cases, the adverse effects of limited-duration availability compromise on agency mission functions and public confidence in the agency can be expected to be limited. In contrast, for time-critical information types, availability is less likely to be restored before serious harm is done to agency assets, operations, or personnel (or to public welfare). As a result of this property, the rationale for most availability impact recommendations will indicate whether or not the information is time-critical.

3.4 Review and Adjustment/Finalization of Information Impact Levels

Particularly where security categorization impact levels recommended in Section 5 or Appendix D are adopted as provisional levels, the agency should review the appropriateness of the default impact levels in the context of the organization, environment, mission, use, and connectivity associated with the system under review. The FIPS 199 criteria presented in Section 3.3 above should be used as the basis for decisions regarding adjustment or finalization of the provisional impact levels. The confidentiality, integrity, and availability impact levels may be adjusted one or more times in the course of the review. Once the review and adjustment process is complete for all information types, the mapping of impact levels by information type can be

finalized. Note that the impact of compromise of information of a particular type can be different in different agencies or in different operational contexts.

3.5 System Security Categorization

Once the impact levels have been selected for individual information types processed by a system, it is necessary to assign a system security category.

3.5.1 FIPS 199 Process for System Categorization

FIPS 199 recognizes that determining the security category of an information system requires additional analysis and must consider the security categories of all information types resident on the information system. For an information system, the potential impact values assigned to each of the respective security objectives (confidentiality, integrity, availability) is the highest values (i.e., high water mark) for any one of these objectives that has been determined for the types of information resident on the information system.[7]

This is in recognition of:

- The fundamental requirement to protect the integrity, availability, and, for at least key information such as passwords and encryption keys, the confidentiality of system-level processing functions and information at the high-water mark in order to achieve that level for any one of the objectives with regard to the information being processed.

- The strong inter-dependence between integrity, confidentiality, and availability.

For this reason, FIPS 199 notes that the value of *not applicable* cannot be assigned to any security objective in the context of establishing a security category for an information system. This is in recognition that there is a low minimum potential impact (i.e., low water mark) on the loss of confidentiality, integrity, and availability for an information system due to the fundamental requirement to protect the system-level processing functions and information critical to the operation of the information system.

The generalized format for expressing the security category, SC, of an information system is:

$$\mathbf{SC}_{\text{information system}} = \{(\mathbf{confidentiality}, \textit{impact}), (\mathbf{integrity}, \textit{impact}), (\mathbf{availability}, \textit{impact})\},$$

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

[7] It is recognized that information systems are composed of both programs and information. Programs in execution within an information system (i.e., system processes) facilitate the processing, storage, and transmission of information and are necessary for the organization to conduct its essential mission-related functions and operations. These system-processing functions also require protection and could be subject to security categorization as well. However, in the interest of simplification, it is assumed that the security categorization of all information types associated with the information system provide an appropriate *worst case* potential impact for the overall information system—thereby obviating the need to consider the system processes in the security categorization of the information system.

SYSTEM EXAMPLE 1: An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. The management within the contracting organization determines that: (i) for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and (ii) for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security categories, SC, of these information types are expressed as:

$$\mathbf{SC}_{\text{contract information}} = \{(\mathbf{confidentiality}, \text{MODERATE}), (\mathbf{integrity}, \text{MODERATE}), (\mathbf{availability}, \text{LOW})\},$$

and

$$\mathbf{SC}_{\text{administrative information}} = \{(\mathbf{confidentiality}, \text{LOW}), (\mathbf{integrity}, \text{LOW}), (\mathbf{availability}, \text{LOW})\}.$$

The resulting security category of the information system is expressed as:

$$\mathbf{SC}_{\text{acquisition system}} = \{(\mathbf{confidentiality}, \text{MODERATE}), (\mathbf{integrity}, \text{MODERATE}), (\mathbf{availability}, \text{LOW})\},$$

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the acquisition system.

SYSTEM EXAMPLE 2: A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. The resulting security categories, SC, of these information types are expressed as:

$$\mathbf{SC}_{\text{sensor data}} = \{(\mathbf{confidentiality}, \text{NA}), (\mathbf{integrity}, \text{HIGH}), (\mathbf{availability}, \text{HIGH})\},$$

and,

$$\mathbf{SC}_{\text{administrative information}} = \{(\mathbf{confidentiality}, \text{LOW}), (\mathbf{integrity}, \text{LOW}), (\mathbf{availability}, \text{LOW})\}.$$

The resulting security category of the information system is initially expressed as:

$$\mathbf{SC}_{\text{SCADA system}} = \{(\mathbf{confidentiality}, \text{LOW}), (\mathbf{integrity}, \text{HIGH}), (\mathbf{availability}, \text{HIGH})\},$$

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the SCADA system. The management at the power plant chooses to increase the potential impact from a loss of confidentiality from low to moderate reflecting a more realistic view of the potential impact on the information system should there be a security breach due to the unauthorized disclosure

of system-level information or processing functions. The final security category of the information system is expressed as:

$$\mathbf{SC}_{\text{SCADA system}} = \{(\textbf{confidentiality}, \text{MODERATE}), (\textbf{integrity}, \text{HIGH}), (\textbf{availability}, \text{HIGH})\}.$$

3.5.2 Guidelines for System Categorization

The impact level for a system will generally be the highest impact level for the security objectives (confidentiality, integrity, and availability) associated with the aggregate of system information types. Yet, an *information system* usually processes several information types, (e.g., privacy information, medical information, proprietary information, financial information, contractor sensitive information). Each of these information types is subject to security categorization. In some cases, the security category for a system will be higher than any impact level for any information type processed by the system. The primary factors that most commonly raise the total system security category above that of its constituent information types are aggregation, connectivity, and critical system functionality. This section provides some general guidelines regarding how aggregation, critical functionality, and some other system factors may affect system security categorization.

Note that variations in sensitivity/criticality with respect to time may need to be factored into the impact assignment process. Some information loses its sensitivity in time (e.g., economic/ commodity projections after they've been published). Other information is particularly critical at some points in time (e.g., weather data in the terminal approach area during aircraft landing operations).

Note also that it may be necessary to involve various stakeholders (e.g., management, operational personnel, or security experts) in decisions regarding system-level impact assessments. Information aggregation, critical system functionality and other factors should be considered in making system-level impact decisions.

3.5.2.1 Aggregation

Some information may have little or no sensitivity in isolation but may be highly sensitive in aggregate. In some cases, aggregation of large quantities of a single information type can reveal sensitive patterns and/or plans, or facilitate access to sensitive or critical systems. In other cases, aggregation of information of several different and seemingly innocuous types can have similar effects. In general, the sensitivity of a given data element is likely to be greater in context than in isolation (e.g., association of an account number with the identity of an individual and/or institution). The availability, routine operational employment, and sophistication of data aggregation and inference tools are all increasing rapidly. If review reveals increased sensitivity or criticality associated with information aggregates, then the system categorization may need to be adjusted to a higher level than would be indicated by the impact associated with any individual information type.

3.5.2.2 Critical System Functionality

Compromise of some information types may have low impact in the context of a system's primary function but may have much more significance when viewed in the context of the potential impact of compromising:

- Other systems to which the system in question is connected or
- Other systems that are dependent on that system's information.

Access control information for a system that processes only low impact information might initially be thought to have only low impact attributes. However, if access to that system might result in some form of access to other systems (e.g., over a network), the sensitivity and criticality attributes of all systems to which such indirect access can result needs to be considered. Similarly, some information may, in general, have low sensitivity and/or criticality attributes. However, that information may be used by other systems to enable extremely sensitive or critical functions (e.g., air traffic control use of weather information or use of commercial flight information in identification aspects of military combat direction systems functionality). Loss of data integrity, availability, temporal context, or other context can have catastrophic consequences.

3.5.2.3 Other System Factors

- ***Web Page Integrity***

  Most Federal government agencies and many organizations within those agencies maintain web pages that are accessible to the public. The vast majority of these public web pages permit interaction between the site and the public. In some cases, the web site provides only information. In other cases, forms may be submitted via the web site (e.g., applications for service or job applications). In some cases, the site is a medium for business transactions. 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 of any agency that operates a public web site. In most cases, the damage can be corrected within a relatively short period of time, and the damage is limited (impact level is ***low***). In other cases (e.g., very large fraudulent transactions, damage to the transaction interface that serves a large population, or modification of a web page belonging to an intelligence/security community component that should be expected to maintain a high level of security), the damage to mission function and/or public confidence in the agency can be serious. In such cases, the integrity impact associated with unauthorized modification or destruction of a public web page would be at least ***moderate***.

- ***Catastrophic Loss of System Availability***

  Either physical or logical destruction of major assets can result in very large expenditures and/or long periods of time for recovery. Permanent loss/unavailability of information system capabilities can seriously hamper

agency operations and, where direct services to the public are involved, have a severe adverse effect on public confidence in Federal agencies. Particularly in the case of large systems, FIPS 199 criteria suggest that catastrophic loss of system's availability would result in a ***high*** availability impact. Whether or not the impact level of system availability should be ***high,*** (and consequent ***high*** system security category) is more a function of the cost and criticality attributes of the system rather than a function of the impact levels for the information types being processed by the system.

- ***Critical Infrastructures and Key National Assets***

  Where the mission served by an information system, or the information that it processes affects the security of critical national infrastructures or key national assets, the harm that can be expected to result from a compromise requires particularly close attention. In this case, an effect on security might include neutralization or significant reduction in effectiveness of physical or cybersecurity protection mechanisms or direct facilitation or implementation of a terrorist attack on critical infrastructures and/or key assets. Accordingly, the impact level should be carefully determined when a loss of confidentiality, integrity, or availability can result in a negative impact on the infrastructure components and assets such as:

  Critical Infrastructures

  - Agriculture and Food (To include farms and food processing plants)
  - Water (To include federal reservoirs and municipal waste water facilities)
  - Public Health (To include hospitals and federal health organization)
  - Emergency Services (Including federal, state, and local response units)
  - Defense Installations and Defense Industrial Base
  - Telecommunications (Including switching and transmission/cable facilities)
  - Energy (Including electric, oil, and gas production and transmission facilities)
  - Transportation (Aviation, rail, highway, pipelines, maritime, and mass transit)
  - Banking/Finance (Including federal services and FDIC insured institutions)
  - Chemical Industry/Hazardous Materials (E.g., chemical plants)
  - Postal and Shipping Facilities

  Key Assets

  - National Monuments and Icons
  - Nuclear Power Plants
  - Dams
  - Government Facilities
  - Commercial Assets

- ***Privacy Information***

  The E-Government Act of 2002 strengthened privacy protection requirements of the *Privacy Act of 1974*. Under the terms of these public laws, Federal government agencies have specific responsibilities regarding collection and dissemination or other disclosure of information regarding individuals. (Note that the OMB definition of individual is a citizen of the United States or an alien lawfully admitted for permanent residence.[8])

  The September 29, 2003 OMB Memorandum, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" puts the privacy provisions of the E-Government Act of 2002 into effect. OMB instructed agency heads "to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected." Under these public laws and executive policies, it is necessary to broaden the definition of "unauthorized disclosure" to encompass *any* sharing of privacy-protected information among Federal government agencies where such sharing is prohibited by privacy laws and policies. Since most privacy regulations focus on sharing or other disclosure of information, most privacy considerations are dealt with in this guideline as special factors affecting the confidentiality impact level. In establishing confidentiality impact levels for each information type, responsible parties must consider the consequences of unauthorized disclosure of privacy information (with respect to violations of Federal policy and/or law).

  OMB acknowledged in its September 2003 memorandum that personal information protection is imperative, given that millions of Americans doing business with their government electronically. OMB guidelines apply to information that identifies individuals in a recognizable form, including name, address, telephone number, Social Security Number, and e-mail addresses.

  Agencies are now required to conduct new Privacy Impact Assessments (PIAs) before developing IT systems that contain identifiable information, or before collecting identifiable information electronically. PIAs must be updated when changes in the way an agency handles personally identifiable information create new privacy risks. Affected agencies are required to report on their e-privacy-related activities every year.

  For their websites, agencies will be required to tell visitors:

  - When it's voluntary to submit information;
  - How to grant consent for agency use of voluntary personal data; and
  - About their rights under the Privacy Act and other such laws.

[8] 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.

Agency websites also will be required to disclose:

- The nature of information collected;
- The purpose and use of such information;
- Whether and to whom the such information will be shared; and
- The privacy safeguards applied to the information collected.

The impact of privacy violations will depend on the penalties associated with violation of the relevant statutes and policies. In most cases, the impacts will fall into the ***low*** to ***moderate*** range. Categorizations should be reviewed to ensure that the consequences of violations have been adequately factored into impact determinations.

4.0 GUIDELINES FOR ASSIGNMENT OF IMPACT LEVELS TO AGENCY-SPECIFIC INFORMATION

This section describes a process for identifying agency-specific information types and for specifying the impact of unauthorized disclosure, modification, or unavailability of this information. Agency-specific information includes both mission information and information associated with the mechanisms that the government uses to achieve its missions. Note that agency-specific information types are, by definition, specific to individual departments and agencies or to relatively constrained sets of departments and agencies. Information types that are common to many departments and agencies are discussed in Section 5, "Impact Levels By Type for Agency-Common Information."

4.1 Identification of Agency-Specific Information Types

The Federal government acquires, generates, processes, and stores a wide variety of information types. The first step in mapping types of Federal information and information systems to security objectives and impact levels is development of an information taxonomy, or creation of a catalog of information types.[9]

Much Federal government information and many information systems are used directly for provision of services. One approach to establishing a set of agency-specific information types at an agency level is to begin by documenting the agency's business or mission areas. Then, the major sub-functions that are necessary to the conduct of each business area or mission area can be defined. For example, one mission conducted by an agency might be law enforcement. Sub-functions that are part of the agency's law enforcement mission might include criminal investigation and surveillance, criminal apprehension, criminal incarceration, citizen protection, crime prevention, and property protection. Each of these sub functions could also represent an information type. Some possible business or mission areas and constituent sub-functions carried out by agency-specific information systems are identified in Appendix D, "Examples of Impact Determination for Agency-Specific Information and Information Systems."

The owner of each system, or an individual designated by the owner, is responsible for identifying the information types stored in, processed by, or generated by that system. In the case of mission information, the responsible individuals, in coordination with management, operational, and security stake holders, should compile a comprehensive set of lines of business and mission areas conducted by the agency, as well as the functions and sub-functions necessary to conduct agency

[9] One issue associated with the taxonomy activity is the determination of the degree of granularity. If the categories are too broad, then the guidelines for assigning impact levels are likely to be too general to be useful. On the other hand, if an attempt is made to provide guidelines for each element of information processed by each government agency, the guideline is likely to be unwieldy and to require excessively frequent changes.

business and/or accomplish agency missions. Each sub-function of a line of business or mission area corresponds to an information type.[10]

4.2 Impact Assessment for Agency-Specific Information

Direct service missions provide the primary frame of reference for determining the impact levels and security objectives for agency-specific information and information systems. The consequences of unauthorized disclosure of information, breach of information or information system integrity, and denial of information or information system services are defined by the nature and beneficiary(ies) of the service being provided or supported. All government agencies perform at least one of the missions and employ at least one of the services delivery mechanisms described in Appendix D. Some perform a number of different missions distributed among several mission areas. Direct service systems process agency-common information (e.g., administrative, management and support information) as well as agency-specific information (e.g., mission information).

Using the impact selection criteria identified in Section 2.2.1 for the security objectives and types of potential losses identified in Section 2.1.2, the entity responsible for impact determination must assign impact levels and consequent security categorization for each agency-specific information type identified for each system. The final system security categorization is based on the impact levels for each information type stored in, processed by, or generated by the system, plus factors that are discussed in Section 3.5.

A factor specific to the confidentiality objective is information subject to special handling (e.g., information subject to the Privacy Act of 1974, 5 U.S.C. § 552A). Regardless of other considerations, some minimum confidentiality impact level must be assigned to any information system that stores, processes, or generates such information. Examples of such information include information subject to the Trade Secrets Act, Privacy Act information, Department of Energy *Safeguards* information, Internal Revenue Service Official Use Only Information, and Environmental Protection Agency Confidential Business Information (e.g., subject to Toxic Substances Control Act; Resource Conservation and Recovery Act; Comprehensive Environmental Response, Compensation, and Liability Act). Some of these statutory and regulatory specifications are listed in Appendix E, "Legislative and Executive Sources Establishing Sensitivity/Criticality."

[10] Appendix C provides an example of Federal government mission information types based on the lines of business and sub-functions identified in the Office of Management and Budget's Federal Enterprise Architecture Program Management Office's *Business Reference Model 2.0*. Note that the appendix is not a part of the basic guideline and the material contained therein is provided for illustration purposes only.

5.0 IMPACT LEVELS BY TYPE FOR AGENCY-COMMON INFORMATION

Much Federal government information and many systems are not employed directly to provide services to citizens, but are primarily intended to manage resources or support delivery of services. This section suggests a set of information types for Federal government information and recommended default security categories for agency-common information types. 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*). The *BRM* describes 39 lines of government business distributed among four business areas. The business areas are high-level categories 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 delivery of services*), and the resource management functions that support all areas of the government's business (*management of resources*). The *support delivery of services* and *management of resources* business areas are together composed of 13 lines of business. The *BRM* subdivides the lines of business into 63 sub-functions. Because the *support delivery of services* and *management of resource* business areas are common to most Federal government agencies, the information associated with each of their 63 sub-functions is identified in this guideline as an agency-common information type.[11] Default confidentiality, integrity, and availability information categories are recommended for each of the 63 agency-common information types. Rationale underlying the recommended default impact level suggestions is provided in Appendix C, "Rationale for Agency-Common Information and Information Systems." Agencies may find it necessary to identify additional information types and assign impact levels to those types.

As with case of agency-specific information, the first step in mapping types of agency-common information and information systems to security objectives and impact levels is to identify the information types stored in, processed by, or generated by the system. Using the criteria identified in Section 2.2.1 in the context of the security objectives identified in Section 2.1.2, the second step is to select the levels of impact and consequent security category for each applicable information type. System security categorization is based on the impact levels associated with each security objective for each type of information stored in, processed by, or generated by the system plus additional factors governing determination of system level impact. (See Section 3.5.) For example, a confidentiality impact level must be assigned to 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

[11] Information types associated with sub-functions of *services for citizens* and *mode of delivery* lines of business are agency-specific and are covered in Section 4, "Guidelines for Assignment of Impact Levels to Agency-Specific Information."

and documentation that may affect access to the information system's data, programs, and/or processes. At least a low confidentiality impact level will apply to this set of information and processes due to a potential for corruption, misuse, or abuse of system information and processes.

Most information systems employed in both service delivery support and resource management activities engage in one or more of the eight italicized *support delivery of services* lines of business identified in Table 2. Each of the 35 information types associated with *support delivery of services* sub-functions is described in Appendix C.1, "Services Delivery Support Functions." These service support functions are the day-to-day activities necessary to provide the critical policy, programmatic, and managerial foundation that support Federal government operations. The direct service missions and constituencies ultimately being supported by service support functions comprise a significant factor in determining the security impacts associated with compromise of information associated with the *support delivery of services* business area.

The *management of government resources* business area includes the back office support activities that enable the Federal government to operate effectively. The five *management of government resources* lines of business are identified in italics in Table 2 under the "Government Resource Management" heading. Each of the 28 information types associated with *management of government resources* sub-functions is described in Appendix C.2, "Government Resource Management Information." 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.

Table 2: Agency-common Lines of Business and Information Types

Services Delivery Support Information		
Controls and Oversight	***Internal Risk Management/Mitigation***	***Revenue Collection***
Corrective Action (Policy/Regulation)	Contingency Planning	Debt Collection
Program Evaluation	Continuity of Operations	User Fee Collection
Program Monitoring	Service Recovery	Federal Asset Sales
Regulatory Development	***Public Affairs***	***Legislative Relations***
Policy & Guidance Development	Customer Services	Legislation Tracking
Public Comment Tracking	Official Information Dissemination	Legislation Testimony
Regulatory Creation	Product Outreach	Proposal Development
Rule Publication	Public Relations	Congressional Liaison
Planning & Resource Allocation		***General Government***
Budget Formulation		Central Fiscal Operations
Capital Planning		Legislative Functions
Enterprise Architecture		Executive Functions
Strategic Planning		Central Property Management
Budget Execution		Central Personnel Management
Workforce Planning		Taxation Management
Management Improvement		Central Reccords & Statistics Management

Table 2: Agency-common Lines of Business and Information Types (Continued)		
Government Resource Management Information		
Human Resources Management	***Information & Technology Mgt***	***Financial Management***
Benefits Management	System Development	Accounting
Personnel Management	Lifecycle/Change Management	Budget and Finance
Payroll Mgt/Expense Reimbursement	System Maintenance	Payments
Resource Training & Development	IT Infrastructure Maintenance	Collections and Receivables
Security Clearance Management	IT Security	Asset and Liability Management
Staff Recruitment & Employment	Record Retention	Reporting and Information
	Information Management	
Administrative Management		***Supply Chain Management***
Facilities/Fleet/Equipment Management		Goods Acquisition
Help Desk Services		Inventory Control
Security Management		Logistics Management
Travel		Services Acquisition
Workplace Policy Development & Mgt		

Table 3 summarizes default impact level recommendations for administrative, management, and service information.

Default impact levels are recommended for each security objective (confidentiality, integrity, availability) for each agency-common Federal government information type. The confidentiality, integrity, and assurance impact levels define the security *category* of each information type.

Most government information systems actually access, process, and/or disseminate more than one class of information. Security objectives and impacts associated with all of the types of information and processes served by the information system need to be considered in determining the system's information security requirements.

Each information type may include one or more of several elements. For example, benefits management information includes employee identification information, benefit plan information for insurance and other products, cost information, claims and reimbursement policy information, claims procedures, etc. In some cases, different impact levels are appropriate for different information elements. For example, elements of program monitoring information relating to remediation of information security vulnerabilities may have a different impact level than elements of program monitoring information relating to an office furniture upgrade. Each agency that processes an information type may process a distinct combination of elements. The authority and responsibilities assigned to each agency that processes an information type can affect the actual impact level associated with the information within the context of that agency's operations.

In addition to rationale for recommended assignments of impact levels to information types, Appendix C of this guideline identifies information elements and contexts that may result in variances from the basic impact level assignment. For example, some systems process information the compromise of which affect national security, critical infrastructures, or key national assets. Impacts associated with such systems are either outside the scope of this document (i.e., national security information) or may need to be adjusted upward based on the

more severe consequences of compromises. Another example is the use of mitigating controls and procedures such as back up and archiving mechanisms and procedures. Use of system and information back-ups and archives can have a significant effect on integrity and availability impacts. Without such mechanisms and procedures, the potential for integrity compromises causing a serious or severe adverse effect on public confidence[12] in the agency is significant for most information types. Similarly, without use of adequate back up and archiving mechanisms and procedures, destructive actions resulting in long-term disruption of access to or use of information systems can have a severe or catastrophic effect on agency missions. Unless there are other factors that force high availability impact, or long-term loss of a particular information type is unlikely to have a serious or catastrophic effect on mission capability, the impact recommendation discussions for integrity and availability impacts are stated as conditional on adequacy, implementation, and use of back-up and archiving mechanisms and procedures.

[12] Note that loss of public confidence may result in impairment of an agency's operational effectiveness.

Table 3: Type-based Impacts for Federal Information and Information Systems			
Security Categorization of Service Delivery Support Information			
	Confidentiality	Integrity	Availability
Controls and Oversight			
Corrective Action	Low	Low	Low
Program Evaluation	Moderate	Low	Low
Program Monitoring	Moderate	Low	Low
Regulatory Development			
Policy and Guidance Development	Moderate	Low	Low
Public Comment Tracking	Low	Low	Low
Regulatory Creation	Moderate	Low	Low
Rule Publication	Low	Low	Low
Planning and Resource Allocation			
Budget Formulation	Moderate	Low	Low
Capital Planning	Low	Low	Low
Enterprise Architecture	Low	Low	Low
Strategic Planning	Low	Low	Low
Budget Execution	Moderate	Moderate	Low
Workforce Planning	Low	Low	Low
Management Improvement	Low	Low	Low
Internal Risk Management and Mitigation			
Contingency Planning	Moderate	Low	Moderate
Continuity of Operations	Moderate	Low	Moderate
Service Recovery	Low	Low	Low
Revenue Collection			
Debt Collection	Moderate	Low	Low
User Fee Collection	Low	Low	Moderate
Federal Asset Sales	Low	Moderate	Low
Public Affairs			
Customer Services	Low	Low	Low
Official Information Dissemination	Low	Low	Low
Product Outreach	Low	Low	Low
Public Relations	Low	Low	Low
Legislative Relations			
Legislation Tracking	Low	Low	Low
Legislation Testimony	Low	Low	Low
Proposal Development	Moderate	Low	Low
Congressional Liason	Moderate	Low	Low
General Government			
Central Fiscal Operations	Moderate	Low	Low
Legislative Functions	Low	Low	Low
Executive Functions	High	Moderate	High
Central Property Management	Low[13]	Low[14]	Low[9]
Central Personnel Management	Low	Low	Low
Taxation Management	Moderate	Low	Low
Central Records and Statistics Management	Moderate	Low	Low

[13] High where safety of major critical infrastructure components or key national assets is at stake and
[14] Moderate or High in emergency situations where time-critical processes affecting human safety or major assets are involved.

Table 3 (Cont'd): Type-based Impacts for Federal Information and Information Systems			
Security Categorization of Government Resource Mangement Functions			
	Confidentiality	Integrity	Availability
Administrative Management			
Facilities, Fleet, and Equipment Management	Low[8]	Low[9]	Low[9]
Help Desk Services	Low	Low	Low
Security Management	Moderate	Moderate	Low
Travel	Low	Low	Low
Workplace Policy Development and Management	Low	Low	Low
Financial Management			
Asset & Liability Management	Low	Low	Low
Reporting & Information	Low	Moderate	Low
Budget & Finance	Moderate	Moderate	Low
Accounting	Low	Moderate	Low
Payments	Low	Moderate	Low
Collections and Receivables	Low	Moderate	Low
Human Resources			
Benefits Management	Low	Low	Low
Personnel Management	Low	Low	Low
Payroll Management and Expense Reimbursement	Low	Low	Low
Resource Training and Development	Low	Low	Low
Security Clearance Management	Moderate	Moderate	Moderate
Staff Recruitment and Employment	Low	Low	Low
Supply Chain Management			
Goods Acquisition	Low	Low	Low
Inventory Control	Low	Low	Low
Logistics Management	Low	Low	Low
Services Acquisition	Low	Low	Low
Information & Technology Management			
System Development	Low	Moderate	Low
Lifecycle/Change Management	Low	Moderate	Low
System Maintenance	Low	Moderate	Low
IT Infrastructure Maintenance	Low	Low	Low
IT Security	Low	Low	Low
Record Retention	Low	Low	Low
Information Management	Low (System High)	Moderate	Low