NIST Special Publication 800-60
Version 2.0

Volume I:
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

June 2004

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 non-governmental 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, Special Publication 800-60
Natl. Inst. Stand. Technol. Spec. Publ. 800-60, Volume I, 57 pages (*June 2004*)

Acknowledgements

The author wishes to thank his colleagues who reviewed drafts of this document and contributed to its development. Special thanks are due to Tanya Brewer-Joneas and Shirley Radack for their careful and thoughtful review. The author also gratefully acknowledges and appreciates the many comments from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Note

NIST Special Publication (SP) 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*, February 2004;
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (Final public draft), April 2004;
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, (Initial public draft), October 2003.
- NIST SP 800-53A, *Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems* (Initial public draft), Fall 2004;
- NIST SP 800-59, *Guideline 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]

This 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 appendixes, including security categorization recommendations for mission-based information types and rationale for security categorization recommendations, are published as a separate volume.

The SP 800-60 information types and security impact levels are based on the OMB Federal Enterprise Architecture Program Management Office's *Business Reference Model 2.0*, inputs from participants in NIST SP 800-60 workshops, and FIPS 199. Rationale for the example impact level recommendations provided in the appendixes have been derived 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 at 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.

[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 is familiar with *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199). The guideline and its appendixes:

- Review the security categorization terms and definitions established by FIPS 199;
- Recommend a security categorization process;
- Describe a methodology for identifying types of Federal information and information systems;
- Suggest provisional security impact levels for common information types;
- Discuss information attributes that may result in variances from the provisional impact level assignment; and
- Describe 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 information associated with administrative activities common to most agencies and information associated with an agency's mission-specific activities. In this guideline, administrative, management, and support information is referred to as *management and support* information. This guideline is less prescriptive for mission-based information than for administrative and support information because there is significantly less commonality of mission information types among agencies than is the case for administrative and support information. While specific administrative and support information types are identified in this guideline, the treatment of mission-based information focuses on general guidelines for identification of information types and assignment of impact levels. (Examples of *management and support* impact assignments are discussed in Appendix C, and examples of mission-based impact assignments 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 appendixes. Users should review the guidelines provided in Volume I, then refer to only that specific material from the appendixes that applies to their own systems and applications.

The provisional impact assignments contained in the appendixes are only the first step in impact assignment and subsequent risk assessment processes. The impact assignments are not intended to be used by auditors as a definitive checklist for information types and impact assignments.

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 *management and support* types. (Although the OMB *BRM* is subject to revision from time to time, not all *BRM* changes will result in changes to the information taxonomy employed in this guideline.)

Some additional information types have been added at the request of Federal agencies. Appendix C recommends provisional confidentiality, integrity, and availability information categories for each *management and support* information type and provides rationale underlying the provisional impact levels. The information types associated with *services to citizens* and *modes of delivery* functions are treated as mission-based information. Recommended provisional impact levels, underlying rationale, and examples of rationale for deviation from the provisional assignments for mission-based 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 (These terms are defined in Appendix A.) 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 SP 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, medical, proprietary, financial, contractor sensitive, trade secret, investigation); and (ii) information systems (e.g., mission critical, mission support, administrative).

Types of information can typically 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 are referred to as *management and support* information. Security attributes of information associated with *mission-based* activities will often vary from agency to agency and can vary among organizations within an agency. This guideline addresses *mission-based* information separately from the more agency-common *management and support* information. Because the consequences of security compromise of mission-based information vary among different operational environments, this guideline is less prescriptive in the case of *mission-based* information than in the case of *management and support* information. Similarly, the specialized knowledge of information types, information use, and program and mission life-cycle context on which the sensitivity of *mission-based* information is dependent is concentrated within the agency responsible for that mission information (or within responsible organizations within agencies). While specific *management and support* information types are defined and discussed the basic guideline, the treatment of *mission-based* information is limited to general guidelines for identification of information types and assignment of impact levels. (Descriptions and provisional impact assignments for both classes of information types are provided in Appendixes C and D, respectively, together with supporting rationale).

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 appendixes, including examples of impact assignments and 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-based* information types and for assignment of security impact levels to mission information; and

- Section 5: Recommended information types for *management and support* information (administrative, management, and service information).

Volume II includes the following appendixes:

- Appendix A: Glossary;

- Appendix B: References;

- Appendix C: Provisional impact assignments and supporting rationale for *management and support* information (administrative, management, and service information);

- Appendix D: Provisional impact assignments and supporting rationale for *mission-based* information (mission information and services delivery mechanisms); 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 assignment and review of provisional impact levels is included in Appendixes 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)

The provisional impact assignments contained in the appendixes are only the first step in impact assignment and should be reviewed in subsequent risk assessment processes. They are not designed to be used by auditors as a definitive checklist for information types and impact assignments.

---

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. [See Public Law 107-347, Section 3542 (b)(2)(A).]

[This page intentionally left blank.]

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 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.

Appendixes to this SP 800-60 guideline recommend provisional impact levels for specific information types. They also provide some rationale for these recommended provisional levels and discuss some of the circumstances that might result in assignment of impact levels higher or lower than the recommended provisional levels.

The impact levels associated with the *management and support* information common to many agencies are strongly affected by the mission-based information with which it is associated. That is, agency-common information used with very sensitive or critical mission-based information types may have higher impact levels than agency-common information used with less critical mission-based information types. Each organization should review the provisional 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.

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

[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.

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 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

The Federal Information Security Management Act 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.

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 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:

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

[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.

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]

[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 Controls and Impact Levels

This subsection provides a step-by-step methodology for mapping information types and information systems to security controls and impact levels. Assignment of security levels is based on FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*. 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.

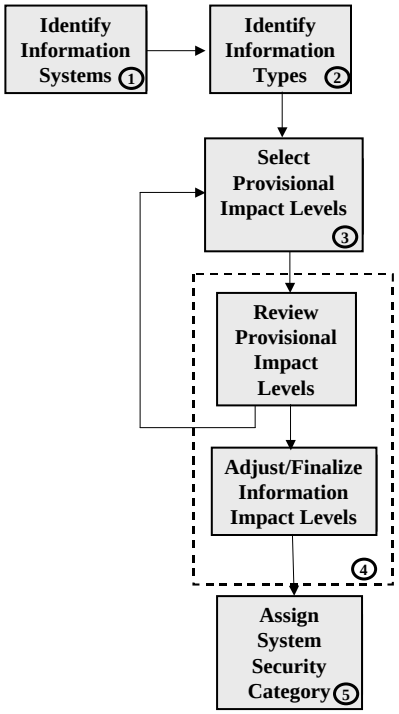

Figure 1: SP 800-60 Security Categorization Process

1. Identify information systems. An information system may be a general support system, a major application, or a local or special purpose system. Agencies should develop their own policies regarding system identification for security categorization purposes. The system is generally bounded by a security perimeter.[7]

2. Identify information types. The user should identify all of the information types that are input, stored, processed, and/or output from each system.[7]

[7] Some assumptions must be made for information types and security perimeters for planned/proposed systems.

3. Select provisional impact levels. The user should select the provisional impact levels for each identified information type. (E.g., see Appendixes C and D.)

4. Review and adjust provisional impact levels. The user should review the appropriateness of the provisional impact levels recommended for the user's information types based on the organization, environment, mission, use, and connectivity associated with the system under review.

   After reviewing the provisional impact levels, adjustments should be made to the 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 as an input to a system risk assessment and selection of the set of security controls necessary for each system. The minimum security controls recommended for each system security category can be found in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

Figure 2 depicts the role of NIST security standards and guidelines in information security programs. The security categorization process documented in these publications feeds the following processes:

- Risk assessment as defined in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, and implemented in the certification and accreditation process as specified in NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

- Selection and implementation of security controls as defined in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* (and the future FIPS of the same title).

- Security planning as specified in NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems* and NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*.

- System certification and accreditation as specified in NIST SP 800-37.

- Impact review for system changes as specified in NIST SP 800-37 and NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*.

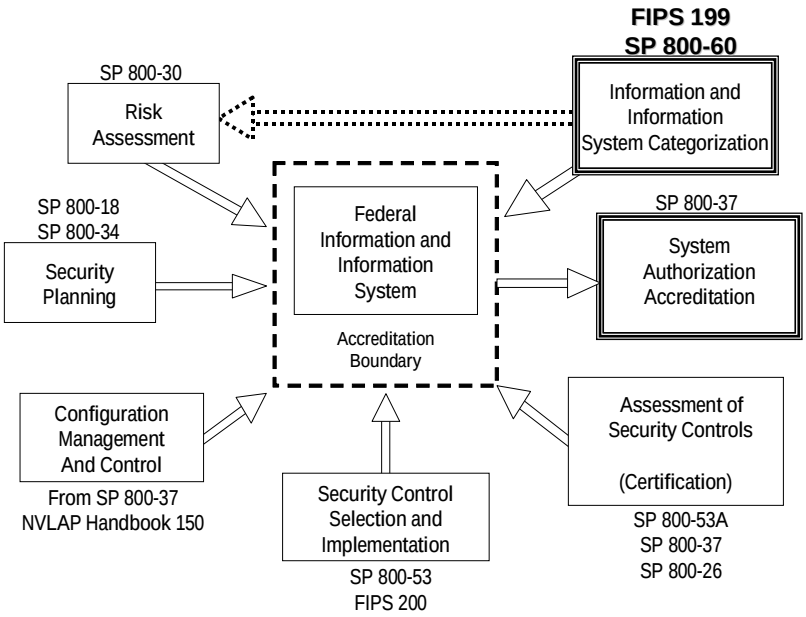

Figure 2: FIPS 199 and SP 800-60 Role in Information Security Program

3.2 Information Type Identification

The following is a suggested methodology that can be employed for identification of information types:

- Identify the fundamental business areas (management and support) or mission areas (mission-based) supported by the system under review;

- Identify, for each business or mission area, the operations 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 operation or line of business;

- Select basic information types associated 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 level.

"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. "Business areas" are subdivided into "areas of operation" or "lines of 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 mission-based. A preliminary list of these mission-based 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. Management and support lines of business that are identified in the Office of Management and Budget's (OMB's) Federal Enterprise Architecture Program Management Office publication, *The Business Reference Model Version 2.0* (*BRM*) are listed in Section 5 of this document. 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 mission-based lines of business are provided in Appendix D. Management and support 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. (Although the OMB *BRM* is subject to revision from time to time, not all *BRM* changes will result in changes to the information taxonomy employed in this guideline.)

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 Version 2.0 of 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

Appendix C suggests provisional confidentiality, integrity, and availability impact levels for management and support information types, and Appendix D provides examples of provisional impact level assignments for some mission-based 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 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 provisional impact levels from Appendix C (for management and support information types) or Appendix D (for mission-based information types). In such cases, the agency should employ the FIPS 199 criteria cited in Table 1, "Categorization of Federal Information and Information Systems," to determine provisional impact levels.

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 prop-rietary 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.

Agencies can assign security categories to information types and information systems by selecting and adjusting appropriate Table 1 values for the potential impact of compromises of confidentiality, integrity, and availability. 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.

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 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 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 of this information type is expressed as:

Security Category $_{\text{administrative information}}$ = {(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 of the information type violate laws, 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 (i) each known variant of the information belonging to the type and (ii) each use of 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 or modifying information to:

- Reduce public confidence in an agency;

- Fraudulently achieve financial gain;

- Create confusion or controversy by promulgating a fraudulent or incorrect procedure;

- Initiate confusion or controversy through false attribution of a fraudulent or false policy;

- Influence personnel decisions;

- Interfere with or manipulate law enforcement or legal processes;

- Influence legislation; or

- 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 is based on the modified information or the modified information is disseminated to other organizations or the public.

Undetected loss of integrity can be catastrophic for 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., facilitation of unauthorized access to sensitive or private information or deny access to information or information system services). Malicious use of 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 systems.

In many cases, the consequences of unauthorized modification 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 in the 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 (i) each known variant of the information belonging to the type and (ii) 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 loss of availability can be catastrophic for many information types. For example, permanent loss of budget execution, contingency planning, continuity of operations, service recovery, debt collection, taxation management, personnel management, payroll management, security management, inventory control, logistics management, or accounting information databases 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 will 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 provisional 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 of this document 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. The impact of compromise of information of a particular type can be different in different agencies or in different operational contexts. Also, the impact for an information type may vary throughout the life cycle. For example, contract information that has a ***moderate*** confidentiality impact level during the life of the contract may have a ***low*** impact level when the contract is completed. Policy information may have ***moderate*** confidentiality and integrity impact levels during the policy development process, ***low*** confidentiality and ***moderate*** integrity impact levels when the policy is implemented, and ***low*** confidentiality and integrity impact levels when the policy is no longer used.

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) are 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.

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.

This is in recognition of:

- The fundamental requirement to protect the integrity, availability, and, for key information such as passwords and encryption keys, the confidentiality of system-level processing functions and information at the high water mark.

- The strong interdependence between integrity, confidentiality, and availability.

For this reason, FIPS 199 notes that, while the value of *not applicable* can apply to specific information types processed by systems, this value cannot be assigned to any security objective for an information system. There is a minimum provisional impact (i.e., low water mark) for a compromise of confidentiality, integrity, and availability for an information system. This is

necessary 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, or *SC*, of an information system is:

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

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

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, or *SC*, of these information types are expressed as:

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

and

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

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

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

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, or *SC*, of these information types are expressed as:

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

and

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

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

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

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:

$$SC_{\text{SCADA system}} = \{(\text{confidentiality, MODERATE}), (\text{integrity, HIGH}), (\text{availability, HIGH})\}.$$

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. An *information system* usually processes several information types, (e.g., privacy, medical, proprietary, financial, contractor sensitive). 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.

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 point in time (e.g., weather data in the terminal approach area during aircraft landing operations).

Various stakeholders (e.g., management, operational personnel, or security experts) may need to be involved 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 to identify military combat transport systems). 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 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. 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 or modification of a web page belonging to an intelligence/security community component), 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 to restore the assets 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 availability may result in a ***high*** availability impact. Whether or not the impact level of system availability should be ***high,*** (and subsequent ***high*** system security category) is dependent on the cost and

criticality attributes of the system rather than on 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 the system processes affects the security of critical national infrastructures or key national assets, the harm that results from a compromise requires particularly close attention. In this case, an effect on security might include a significant reduction in the effectiveness of physical or cybersecurity protection mechanisms, or facilitation 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 will result in a negative impact on the infrastructure components and assets such as:

Critical Infrastructures

- Agriculture and Food (Including farms and food processing plants)
- Water (Including federal reservoirs and municipal waste water facilities)
- Public Health (Including hospitals and federal health organizations)
- 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

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

The *Critical Information Infrastructure Act of 2002*, Public Law 107-296 §§ 211-215 of November 25, 2002 (codified as 6 U.S.C. 131-134), defines the term "critical infrastructure information" to mean information not customarily in the public domain and related to the security of critical infrastructure or protected systems. Under the act, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as defined by the law:

(1) Shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);
(2) Shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;
(3) Shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;
(4) Shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this law[8];
(5) Shall not, if provided to a State or local government or government agency, be made available pursuant to any State or local law requiring disclosure of information or records, otherwise be disclosed or distributed to any party by a State or local government or government agency without the written consent of the person or entity submitting such information, or be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act; and

Does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

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, dissemination or disclosure of information regarding individuals.[9]

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. The guidance applies to information that identifies individuals in a recognizable form, including name, address, telephone number, Social Security Number, and e-mail addresses. 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 disclosing information, privacy considerations are dealt with in this guideline as special factors affecting the confidentiality impact level. In establishing confidentiality impact levels for each

[8] Except in furtherance of an investigation or the prosecution of a criminal act, or when disclosure of the information would be to either House of Congress or to the Comptroller General in the course of the performance of the duties of the General Accounting Office.

[9] The Office of Management and Budget (OMB) definition of individual is, "a citizen of the United States or an alien lawfully admitted for permanent residence." Agencies may choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.

information type, responsible parties must consider the consequences of unauthorized disclosure of privacy information (with respect to violations of Federal policy and/or law). In addition, there are four management and support information types that address privacy information.

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 applicable laws.

Agency websites will be required to disclose:

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

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

Trade Secrets

There are several laws that specifically prohibit unauthorized disclosure of trade secrets (e.g., 7 U.S.C., Chapter 6, Subchapter II, Section 136h and 42 U.S.C., Chapter 6A, Subchapter XII, Part E, Section 300j-4(d)(1)). Systems that store, communicate, or process trade secrets will generally be assigned at least a ***moderate*** confidentiality impact level.

[This page intentionally left blank.]

4.0 GUIDELINES FOR ASSIGNMENT OF IMPACT LEVELS TO MISSION-BASED INFORMATION

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

4.1 Identification of Mission-based 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 the development of an information taxonomy, or creation of a catalog of information types.[10]

Much Federal government information and many information systems are used directly for the provision of services. One approach to establishing mission-based information types at an agency level is to begin by documenting the agency's business and mission areas. Then, the major sub-functions that are necessary to the conduct of each business and 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 business and mission areas and constituent sub-functions carried out by mission-based information systems are identified in Appendix D, "Examples of Impact Determination for Mission-based 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-based 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 business and/or accomplish agency missions. Each sub-function of a line of business or mission area corresponds to an information type.[11]

---

[10] 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.

[11] Appendix D provides 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*.

4.2 Impact Assessment for Mission-based Information

Direct service missions provide the primary frame of reference for determining the impact levels and security objectives for mission-based information and information systems. The consequences of unauthorized disclosure of information, breach of integrity, and denial of 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 *management and support* information as well as mission-based 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 mission-based 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.”

5.0 IMPACT LEVELS BY TYPE FOR MANAGEMENT AND SUPPORT 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 recommends a set of information types for Federal government information. Recommended provisional security categories for *management and support* information types, together with supporting rationale are presented in Appendix C. As stated in Section 4, the basis 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*);
- Mechanisms the government uses to achieve its purpose (*modes of delivery*);
- Support functions necessary to conduct government (*support delivery of services*); and
- 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. The *support delivery of services* and *management of resource* business areas are common to most Federal government agencies, and the information associated with each of their sub-functions is identified in this guideline as a *management and support* information type.[12] Four additional *management and support* information types have been defined that address privacy information. One additional *management and support* information type has been defined that addresses executive function information. Provisional confidentiality, integrity, and availability information categories are recommended in Appendix C for all of the *management and support* information types. Rationale underlying the recommended provisional impact level suggestions is also provided in Appendix C. Agencies may find it necessary to identify additional information types and assign impact levels to those types.

As with case of mission-based information, the first step in mapping types of *management and support* 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 next 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

[12] 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 Mission-Based Information."

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, configuration and security policy enforcement information includes password files, network access rules, other hardware and software configuration settings, and documentation that may affect access to the information system's data, programs, and/or processes. At a minimum, 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.

Table 2 lists the *management and support* lines of business and information types.

Table 2: Management and support Lines of Business and Information Types

Services Delivery Support Information

Controls and Oversight
Corrective Action (Policy/Regulation)
Program Evaluation
Program Monitoring

Regulatory Development
Policy & Guidance Development
Public Comment Tracking
Regulatory Creation
Rule Publication

Planning & Resource Allocation
Budget Formulation
Capital Planning
Enterprise Architecture
Strategic Planning
Budget Execution
Workforce Planning
Management Improvement

Internal Risk Management/Mitigation
Contingency Planning
Continuity of Operations
Service Recovery

Public Affairs
Customer Services
Official Information Dissemination
Product Outreach
Public Relations

Revenue Collection
Debt Collection
User Fee Collection
Federal Asset Sales

Legislative Relations
Legislation Tracking
Legislation Testimony
Proposal Development
Congressional Liaison

General Government
Central Fiscal Operations
Legislative Functions
Executive Functions
Central Property Management
Central Personnel Management
Taxation Management
Central Records & Statistics Management
Income Information
Personal Identity and Authentication
Entitlement Event Information
Representative Payee Information

Government Resource Management Information

Human Resources Management
Benefits Management
Personnel Management
Payroll Mgt/Expense Reimbursement
Resource Training & Development
Security Clearance Management
Staff Recruitment & Employment

Administrative Management
Facilities/Fleet/Equipment Management
Help Desk Services
Security Management
Travel
Workplace Policy Development & Mgt

Information & Technology Mgt
System Development
Lifecycle/Change Management
System Maintenance
IT Infrastructure Maintenance
IT Security
Record Retention
Information Management

Financial Management
Accounting
Budget and Finance
Payments
Collections and Receivables
Asset and Liability Management
Reporting and Information

Supply Chain Management
Goods Acquisition
Inventory Control
Logistics Management
Services Acquisition

5.1 Services Delivery Support Information

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 information types associated with *support delivery of services* sub-functions is described below. Appendix C.2, "Services Delivery Support

Functions," recommends provisional impact levels for confidentiality, integrity, and availability. 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.

5.1.1 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.

5.1.1.1 Corrective Action Information Type

Corrective Action information supports the enforcement functions necessary to remedy programs that have been found non-compliant with a given law, regulation, or policy. In most cases, the confidentiality, integrity and availability impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.1.2 Program Evaluation Information Type

Program Evaluation information supports the analysis of internal and external program effectiveness and the determination of corrective actions as appropriate. In most cases, the confidentiality, integrity and availability impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of program evaluation information on the abilities of responsible agencies to analyze internal and external program effectiveness and to determine appropriate corrective actions.

5.1.1.3 Program Monitoring Information Type

Program Monitoring information supports the data-gathering activities required to determine the effectiveness of internal and external programs and the extent to which they comply with applicable laws, regulations, and policies. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of program monitoring information on the ability of responsible agencies to perform data-gathering activities. These activities determine the effectiveness of internal and external programs and the extent to which they comply with related laws, regulations, and policies.

5.1.2 Regulatory Development

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

5.1.2.1 Policy and Guidance Development Information Type

Policy and Guidance Development information supports 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. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.2.2 Public Comment Tracking Information Type

Public Comment Tracking information supports the activities of soliciting, maintaining, and responding to public comments regarding proposed regulations. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of public comment tracking information on the ability of responsible agencies to solicit, maintain, and respond to public comments regarding proposed regulations.

5.1.2.3 Regulatory Creation Information Type

Regulatory Creation information supports the activities of researching and drafting proposed and final regulations. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of regulatory creation information on the ability of responsible agencies to research and draft proposed and final regulations.

5.1.2.4 Rule Publication Information Type

Rule Publication information supports all the activities associated with the publication of a proposed or final rule in the Federal Register and Code of Federal Regulations. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.3 Planning and Resource Allocation

Planning and Resource Allocation information supports 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.

5.1.3.1 Budget Formulation Information Type

Budget Formulation information supports 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. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.3.2 Capital Planning Information Type

Capital Planning information supports the processes for ensuring that appropriate investments are selected for capital expenditures. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of capital planning information on the ability of responsible agencies to ensure that appropriate investments are selected for capital expenditures.

5.1.3.3 Enterprise Architecture Information Type

Enterprise Architecture information supports an established process for describing the current state and defining the target state and transition strategy for an organization's people, processes, and technology. In most cases, the confidential impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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 organization's people, processes, and technology.

5.1.3.4 Strategic Planning Information Type

Strategic Planning information supports the determination of long-term goals and the identification of the best approach for achieving those goals. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.3.5 Budget Execution Information Type

Budget Execution information supports the day-to-day requisitions and obligations for agency expenditures, invoices, billing dispute resolution, reconciliation, service level agreements, and distributions of shared expenses. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.3.6 Workforce Planning Information Type

Workforce Planning information supports the processes for identifying the workforce competencies required to meet the agency's strategic goals and for developing the strategies to meet these requirements. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.3.7 Management Improvement Information Type

Management Improvement information supports all efforts to gauge the ongoing efficiency of business processes and identify opportunities for reengineering or restructuring. In most cases, the confidential impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.4 Internal Risk Management and Mitigation

Internal Risk Management and Mitigation information supports all activities relating to the processes of analyzing exposure to risk and determining appropriate counter-measures. Risks to much information associated with 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.

5.1.4.1 Contingency Planning Information Type

Contingency Planning information supports the actions required to plan for, respond to, and mitigate damaging events. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of contingency planning information on the ability of responsible agencies to plan for, respond to, and mitigate damaging events.

5.1.4.2 Continuity of Operations Information Type

Continuity of Operations information supports 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. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.4.3 Service Recovery Information Type

Service Recovery information supports the internal actions necessary to develop a plan for resuming operations after a catastrophe occurs, such as a fire or earthquake. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.5 Public Affairs

Public Affairs information supports activities involving 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.

5.1.5.1 Customer Services Information Type

Customer Service information supports activities associated with providing and managing the delivery of information and support to the government's customers. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.5.2 Official Information Dissemination Information Type

Official Information Dissemination information supports efforts to provide official government information to external stakeholders through the use of various types of media (e.g., video, paper, web, etc.). In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.5.3 Product Outreach Information Type

Product Outreach information supports 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. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.5.4 Public Relations Information Type

Public Relations information supports the efforts to promote an organization's image through the effective handling of citizen concerns. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of public relations information on the ability of responsible agencies to promote an organization's image through the effective handling of citizen concerns.

5.1.6 Revenue Collection

Revenue Collection information 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.

5.1.6.1 Debt Collection Information Type

Debt Collection information supports activities associated with the collection of money owed to the United States government from both foreign and domestic sources. In most cases, the confidentiality, integrity and availability impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.6.2 User Fee Collection Information Type

User Fee Collection information supports 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). In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.6.3 Federal Asset Sales Information Type

Federal Asset Sales information supports 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. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.7 Legislative Relations

Legislative Relations information supports activities aimed at the development, tracking, and amendment of public laws through the legislative branch of the Federal government.

5.1.7.1 Legislation Tracking Information Type

Legislation Tracking information supports following legislation from conception to adoption. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of legislation tracking information on the ability of responsible agencies to follow legislation from conception to adoption.

5.1.7.2 Legislation Testimony Information Type

Legislation Testimony information supports activities associated with providing testimony/evidence in support of, or opposition to, legislation from conception to adoption. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of legislation testimony information on the ability of responsible agencies to provide testimony/evidence in support ofr, or opposition to, legislation from conception to adoption.

5.1.7.3 Proposal Development Information Type

Proposal Development information supports drafting proposed legislation that creates or amends laws subject to Congressional legislative action. In most cases, the impact levels are based on

the effects of unauthorized disclosure, modification, or loss of availability of proposal development information on the ability of responsible agencies to draft proposed legislation that creates or amends laws subject to Congressional legislative action.

5.1.7.4 Congressional Liaison Information Type

Congressional Liaison Operations information supports all activities associated with supporting the formal relationship between a Federal Agency and the U.S. Congress. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of Congressional liaison information on the ability of responsible agencies to support their formal relationships with the U.S. Congress.

5.1.8 General Government

General Government information supports 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. Generally, all activities 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. However, unlike other service support functions, some general government information types are associated with specific organizations (e.g., Office of Personnel Management for central personnel management).

5.1.8.1 Central Fiscal Operations Information Type

Central Fiscal Operations information supports the fiscal operations performed by a designated organization(s) on behalf of the Government.[13] In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of central fiscal operations information on the fiscal operations that are performed on behalf of the Government by a designated organization(s). Impacts to some information and information systems associated with central fiscal operations may affect the security of the critical banking and finance infrastructure. The potential for consequent loss of human life or of major national assets is typically low.

5.1.8.2 Legislative Functions Information Type

Legislative Functions information supports 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. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

[13] Tax-related functions are associated with the Taxation Management information type.

5.1.8.3 Executive Functions Information Type

Executive Functions[14] information supports the operations of the Executive Office. The impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of the executive information type on functions of the Executive Office

5.1.8.4 Central Property Management Information Type

Central Property Management information supports most of the operations of the General Services Administration. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.8.5 Central Personnel Management Information Type

Central Personnel Management information supports most of the operating activities of the Office of Personnel Management (OPM) and related agencies. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of central personnel management information on the ability of the Office of Personnel Management 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.

5.1.8.6 Taxation Management Information Type

Taxation Management information supports activities associated with the implementation of the Internal Revenue Code and the collection of taxes in the United States and abroad. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of taxation management information on the ability of designated agencies to enforce the Internal Revenue Code and to collect taxes in the United States and abroad.

5.1.8.7 Central Records and Statistics Management Information Type

Central Records and Statistics Management information supports 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 the National Archives and Records Administration (NARA) or the statistics and data collection performed by the Department of Commerce.[15] In most cases, the

[14] In the OMB Business Reference Model "Executive Function" has been expanded to include general agency executive functions as well as Executive Office of the President (EOP) functions. Strictly EOP executive functions are treated in Appendix D, Examples of Impact Determination for Mission-Based Information and Information Systems.

[15] 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

impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.1.8.8 Income Information

Income information supports all the wages, self employment earnings, savings type data and other financial resources information that are needed to help determine the amount of Retirement, Survivor, or Disability benefits that individuals may be entitled to receive or not receive from the Supplementary Security Income or RSDI Title II Programs. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of income information on the ability of the Federal government to identify citizen entitlements and obligations and to protect individuals against identity theft and the Federal government against fraud.

5.1.8.9 Personal Identity and Authentication Information

Personal identity and authentication information includes that information necessary to ensure that all persons who are potentially entitled to receive any federal benefit are enumerated and identified so that Federal agencies can have reasonable assurance that they are paying or communicating with the right individuals. This information include individual citizen's Social Security Numbers, names, dates of birth, places of birth, parents' names, etc.[16] In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of personal identity and authentication information on the ability of Federal agencies to determine that communications with and payments to individuals are being made with or to the correct individuals.

5.1.8.10 Entitlement Event Information

Entitlement Event information includes information about events such as death and date of occurrence, date of a disabling event and the relating data that can reasonably prove the severity of such disability, proof of age for retirement benefits, birth and relationship of spouse and/or children who may be entitled to benefits only as auxiliaries of the primary beneficiary, and other related information needed to process a claim for benefits. This also includes means-related information required to administer all the means-related benefits associated with the Title XVI (Supplementary Security Income Program) and the new drug provisions of the recently revised Medicare Program. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of entitlement event information on the ability of the Federal government to establish qualifications of individuals to receive government benefits.

---

records and statistics management information type is intended for functions performed on behalf of the entire Federal government.

[16] Persons conducting sensitive or payment related business with the government must identify themselves to the level prescribed by appropriate governing directives using such data.

5.1.8.11 Representative Payee Information

Representative Payee information includes information required to determine the need for representative payees and the data that is gathered to make the determination of who should serve as the representative payee for all beneficiaries of federal benefits who are unable to manage their own funds. This also includes accountability information required to provide reasonable assurance that the funds are being used appropriately for the well-being of entitled individuals. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of representative payee information on the ability of the Federal government to determine that entitlement funds are being used appropriately for the well-being of entitled individuals.

5.2 Government Resource Management Information

The *government resources management information* business area includes the back office support activities that enable the Federal government to operate effectively. The five *government resources management information* lines of business are identified in italics in Table 2 under the "Government Resource Management" heading. Each of the information types associated with *government resources management information* sub-functions is described below. Appendix C.3, "Government Resource Management Information," recommends provisional impact levels for confidentiality, integrity, and availability compromises of services delivery support 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 nature of the supported direct services and constituencies being supported.

5.2.1 Human Resources Management

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

5.2.1.1 Benefits Management Information Type

Benefits Management information supports the administration of entitled benefits for federal personnel such as retirement, medical, disability, and insurance. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of benefits management information on the abilities of responsible agencies to administer entitled benefits for federal personnel such as retirement, medical, disability, and insurance.

5.2.1.2 Personnel Management Information Type

Personnel Management information supports the general management of the federal workforce, including functions such as personnel action processing, employee tracking, position classification and management, discipline/grievance, advancement and awards, and labor relations. In most cases, the impact levels are based on the effects of unauthorized disclosure,

modification, or loss of availability of personnel management information on the abilities of responsible agencies to manage the federal workforce.

5.2.1.3 Payroll Management and Expense Reimbursement Information Type

Payroll Management and Expense Reimbursement information supports the administration and determination of federal employee compensation.[17] In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of payroll management and expense reimbursement information on the ability of responsible agencies to administer and determine Federal employee compensation.

5.2.1.4 Resource Training and Development Information Type

Resource Training and Development information supports the active building of capacities in staff members through formal education, technical training, or other means of education. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.2.1.5 Security Clearance Management Information Type

Security Clearance Management information supports 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. Impacts to some information and information systems associated with security clearance management may affect the security of critical infrastructures and key national assets. Also, although much information associated with security clearance management is national security related (outside the scope of this guideline); security clearance management, as used in this guideline, is not restricted to national security applications. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.2.1.6 Staff Recruitment and Employment Information Type

Staff Recruitment and Employment information supports the active marketing and hiring of personnel to fill opportunities and vacancies within an organization. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

[17] See *payments* information type for the actual payment of salary and expenses.

5.2.2 Administrative Management

Administrative Management information supports the day-to-day management and maintenance of the internal infrastructure. Administrative information is usually routine and is relatively low impact. However, some administrative management information is either very 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). All *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.

5.2.1.1 Facilities, Fleet, and Equipment Management Information Type

Facilities, Fleet, and Equipment Management information supports the maintenance, administration, and operation of offices buildings, fleets, machinery, and other capital assets considered as possessions of the Federal government. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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. Impacts to some information and information systems associated with facilities, fleet, and equipment management may affect the security of some key national assets (e.g., nuclear power plants, dams, and other government facilities).

5.2.2.2 Help Desk Services Information Type

Help Desk Services information supports the management of a service center to respond to government employees' technical and administrative questions. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of help desk service information on the ability of responsible agencies to manage service center responses to government employees' technical and administrative questions.

5.2.2.3 Security Management Information Type

Security Management information supports the physical protection of an organization's personnel, assets, and facilities. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of security management information on the ability of responsible organizations to physically protect their personnel, assets, and facilities. Impacts to some information and information systems associated with security management may 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 potential threat to human life associated with the asset(s) being protected. For example, the impact levels may be based on the consequences to the public of terrorist access to dams or nuclear power plants.

5.2.2.4 Travel Information Type

Travel information supports the activities associated with planning, preparing, and monitoring of business related travel for an organization's employees. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of travel information on the abilities of responsible agencies to plan, prepare, and monitor business related travel for the organization's employees.

5.2.2.5 Workplace Policy Development and Management Information Type (*Intra-Agency Only*)

Workplace Policy Development and Management information supports all activities required to develop and disseminate workplace policies such as dress codes, time reporting requirements, telecommuting, etc. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.2.3 Information and Technology Management

Information and Technology Management information supports the coordination of information technology (IT) 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. In contrast, integrity and availability protection cannot be maintained for copies of information that have been distributed to the public. Only by maintaining copies of information in organization-controlled information systems can integrity and availability assurance be maintained.

5.2.3.1 System Development Information Type

System Development information supports all activities associated with the in-house design and development of software applications. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of system development information on the ability of responsible agencies to design and develop software applications in-house.

5.2.3.2 Lifecycle/Change Management Information Type

Lifecycle/Change Management information supports 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. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of lifecycle/change management information on the ability of responsible agencies to 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.

5.2.3.3 System Maintenance Information Type

System Maintenance information supports all activities associated with the maintenance of in-house designed software applications. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of system maintenance information on the ability of responsible agencies to maintain in-house designed software applications.

5.2.3.4 IT Infrastructure Management Information Type

IT Infrastructure Maintenance information supports 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 (including implementing files and/or switch settings), hardware and software configuration settings, and documentation that may affect access to the information system's data, programs, and/or processes. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.). The impact levels associated with IT infrastructure maintenance information are primarily a function of the information processed in the infrastructure. (See also 5.2.3.5, IT Security Information and 5.2.3.7, Information Management Information.) IT infrastructure maintenance also includes information systems configuration and security policy enforcement information.

5.2.3.5 IT Security Information Type

IT Security information supports 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. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.2.3.6 Record Retention Information Type

Records Retention information supports the operations surrounding the management of the official documents and records for an agency. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of record retention information on the ability of responsible organizations to store, track, account for, maintain, retrieve, and disseminate official documents and records. *National security information* and *national security systems* are outside the scope of this guideline.

5.2.3.7 Information Management Information Type

Information Management information supports the coordination of information collection, storage, dissemination, and destruction as well as managing the policies, guidelines, and standards regarding information management. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of information management information on the ability of responsible agencies to perform the day-to-day processes of information collection, storage, dissemination, and destruction and managing the policies, guidelines, and standards regarding information management.

5.2.4 Financial Management

Financial Management information supports 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 specific projects, programs, and/or technologies that might be revealed by unauthorized disclosure of information. Integrity breaches such as successful frauds can affect agency image. Permanent loss/unavailability of financial management information can cripple agency operations.

5.2.4.1 Assets and Liability Management Information Type

Assets and Liability Management information provides 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. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.2.4.2 Reporting and Information Information Type

Reporting and Information information provides financial information, reporting and analysis of financial transactions. Financial reporting information supports 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. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of financial reporting information on an agency's ability to provide financial information and reporting and analysis of financial transactions.

5.2.4.3 Budget and Finance Information Type

Budget and Finance information supports 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 information supports the establishment of a system for ensuring an organization does not obligate or disburse funds in excess of those appropriated or authorized. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.2.4.4 Accounting Information Type

Accounting information supports accounting for assets, liabilities, fund balances, revenues and expenses associated with the maintenance of Federal funds and expenditure of Federal appropriations (e.g., salaries and expenses, operation and maintenance, procurement, working capital, trust funds, etc.), in accordance with applicable Federal standards (e.g., FASAB, Treasury, OMB, GAO, etc.). In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of accounting information on the abilities of government agencies to maintain Federal funds and expenditure of Federal appropriations in accordance with applicable Federal standards.

5.2.4.5 Payments Information Type

Payments information includes 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. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of payments information on the ability of responsible agencies to provide appropriate control over all payments made by or on behalf of an organization.

5.2.4.6 Collections and Receivables Information Type

Collections and Receivables information includes 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. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.2.5 Supply Chain Management

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

5.2.5.1 Goods Acquisition Information Type

Goods Acquisition information supports the procurement of physical goods, products, and capital assets to be used by the Federal government. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of goods acquisition information on the ability of agencies to procure physical goods, products, and capital assets to be used by the Federal government.

5.2.5.2 Inventory Control Information Type

Inventory Control information supports the tracking of information related to procured assets and resources with regards to quantity, quality, and location. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability 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.

5.2.5.3 Logistics Management Information Type

Logistics Management information supports the planning and tracking of personnel and their resources in relation to their availability and location. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of logistics management information on the ability of agencies to plan and track the availability and location of personnel and their resources.

5.2.5.4 Services Acquisition Information Type

Services Acquisition information supports the oversight and/or management of contractors and service providers from the private sector. In most cases, the impact levels are based on the effects of unauthorized disclosure, modification, or loss of availability of services acquisition information on the ability of agencies to oversee and manage contractors and service providers from the private sector.