ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

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

By William C. Barker
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Introduction

In response to the requirements of Title III of the E-Government Act (Public Law 107-347), titled the Federal Information Security Management Act (FISMA), ITL recently published NIST Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*. Summarized in this *ITL Bulletin*, the guide was developed to assist federal government agencies to categorize information and information systems with respect 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. SP 800-60 applies to all federal systems other than *national security systems* as defined in FISMA and NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*. SP 800-60 and its appendices:

- Review the security categorization terms and definitions established by Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- 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;
- Identify 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.

SP 800-60 is intended as a reference resource rather than as a tutorial. Not all of the material will be relevant to all agencies. SP 800-60 includes two volumes: Volume I is a basic guideline and Volume II contains appendices. Users should review the guidelines provided in Volume I, then refer to only the material from the appendices that is applicable.

The *provisional* impact assignments contained in the appendices 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 primary source for the 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*),
- Mechanisms the government uses to achieve its purpose (*modes of delivery*),
- Support functions necessary to conduct government (*support services*), and
- 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 included in the *management and support* types. Some additional information types have

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since March 2003

been added at the request of federal agencies. The information types associated with *services to citizens* and *modes of delivery* functions are included in the *mission-based* information types.

Volume II lists legal and executive sources that establish sensitivity and/or criticality characteristics for specific types of information processed by the federal government. Citations from the United States Code and Executive Orders are listed in Appendix E.

Security Categorization of Information and Information Systems

FIPS 199 defines the security categories, security objectives, and impact levels to which SP 800-60 maps information types. FIPS 199 also describes the context of use for this guideline.

The impact levels for the *management and support* information common to many agencies are strongly affected by the *mission-based* information with which it is associated. 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.

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.

FIPS 199 establishes three impact levels relevant to securing federal information for three security objectives (confidentiality, integrity, and availability). A loss of *confidentiality* is the unauthorized disclosure of information. A loss of *integrity* is the unauthorized modification or destruction of information. A loss of *availability* is the disruption of access to or use of information or an information system. The generalized format for expressing the security category, or *SC*, of an information type is:

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

where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE.

Mapping Information Types to Security Controls and Impact Levels

SP 800-60 specifies the following step-by-step methodology for mapping information types and information systems to security controls and impact levels:

- *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.
- *Identify information types*. The user should identify all of the information types that are input, stored, processed, and/or output from each system.
- *Select provisional impact levels*. The user should select the provisional impact levels for each identified information type from Appendices C and D.
- *Review and adjust provisional impact levels*. The user should review the appropriateness of the provisional impact levels recommended for each information type 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.
- *Assign system security category*. The user establishes the level of confidentiality, integrity, and availability impacts 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.

Following completion of the system security categorization process, the resulting impact level can be used as an input to a system risk assessment and in selection of the security controls necessary for each system. The minimum security controls recommended for each system security category will be found in DRAFT NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

Information Type Identification

SP 800-60 suggests a 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 subfunctions necessary to carry out each area of operation or line of business;
- Select basic information types associated with the identified subfunctions; 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.

Who we are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov/.

Once a set of information types has been selected, the agency should review the information processed by the system to see if additional types need to be identified for impact assessment purposes.

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 levels 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. An agency may identify information types not listed in SP 800-60 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 following criteria to determine provisional impact levels.

– 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.

– 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.

– 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.

Review and Adjustment/ Finalization of Information Impact Levels

Particularly where security categorization impact levels recommended in 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 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.

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. 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. The potential impact values assigned to each security objective (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.

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:

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

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

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). Other factors that SP 800-60 addresses with respect to making system-level impact decisions include aggregation, critical system functionality, web page integrity, catastrophic loss of system availability, critical infrastructures and key national assets, privacy information, and trade secrets.

NIST SP 800-60 is available for download at our Computer Security Resource Center at http://csrc.nist.gov /publications/. Other publications mentioned in this bulletin are also available at this website.

ITL Bulletins Via E-Mail
We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900