Establishing System Security Level Procedures and Guidelines

A Mandatory Reference for ADS Chapter 545

New Reference: 06/01/2006
Responsible Office: M/DCIO
File Name: 545man_060106_cd44

Information System Security
Establishing Security Level Procedures and Guidelines
for System Owners

1. Introduction

This document defines the procedures and guidelines that you must follow when establishing a security level for a USAID information system.

2. Security Level

As a System Owner, you derive your information system's security level from the potential impact on USAID should a breach in security occur that jeopardizes the information system or the information contained within it. The three evaluation criteria, confidentiality, integrity, and availability (known as security objectives), are used to define the level of potential impact. You determine the security level by measuring the potential impact on the information system from the loss of each of these objectives through the following processes:

- Identify the information system.
- Identify the information types it handles.
- Determine the security level for each information type, in terms of potential impact values.
- Determine the overall security level (the aggregate of the individual scores).
- Assign the information system security level.

The resulting security level information is used in other processes, such as risk assessment, security controls selection, and certification and accreditation.

3. Security Objectives

The Federal Information Security Management Act (FISMA) and Federal Information Processing Standard (FIPS) Publication 199 define three security objectives for information and information systems:

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

- **Integrity** "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]
- **Availability** "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

You must evaluate the three security objectives in terms of the potential impact to the information system if the assurances were lost or compromised.

4. Potential Impact

The potential impact is the effect on a USAID information system should there be a loss or compromise of the security objective. You may evaluate individual potential impacts to one of the following four values: Low, Moderate, High, and Not Applicable. You may assign the Not Applicable value only when there is no potential impact for the loss or compromise of the security objective (confidentiality: protection of public information on a public web server would rate N/A). For information systems, you cannot assign the Not Applicable value; at a minimum, you must always assign a potential impact of Low to a USAID information system.

You may assign a **Low** value as a potential impact if the loss or compromise of the security objective would have a limited adverse effect. A limited adverse effect means that the loss of confidentiality, integrity, or availability might cause: (a) the organization to perform its primary functions in a noticeably reduced capacity; (b) minor damage to organizational assets; (c) minor financial loss; or (d) minor harm to individuals.

You may assign a **Moderate** value as a potential impact if the loss or compromise of the security objective would have a serious adverse effect. A serious adverse effect means that the loss of confidentiality, integrity, or availability might cause: (a) the organization to perform its primary functions in a significantly reduced capacity; (b) significant damage to organizational assets; (c) significant financial loss; or (d) significant harm to individuals, but not loss of life or life-threatening injuries.

You may assign a **High** value as a potential impact if the loss or compromise of the security objective would have a severe or catastrophic adverse effect. A severe or catastrophic adverse effect means that the loss of confidentiality, integrity, or availability might cause: (a) the organization to be unable to perform its primary functions; (b) major damage to organizational assets; (c) major financial loss; or (c) severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

The following table summarizes the potential impact definitions for each security objective:

	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality	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/ assets, or individuals.
Integrity	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/ assets, or individuals.
Availability	The disruption of access to or use of information 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 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 could be expected to have a **severe or catastrophic** adverse effect on organizational operations/ assets, or individuals.

This table is a three by three matrix that takes the security objective and the potential impact and provides a summarization of the potential impact. You use the individually evaluated and assigned potential impacts to determine the security level for the information system, which is an aggregate of the individual scores.

5. Security Level for Information Types

Prior to determining the security level of the information system, you must determine the security level of the information handled by the system. The information can be broken down into various types, corresponding to the system's business functions. (See NIST 800-60)

For each type of information, you must determine the effect on USAID should there be a loss or compromise of each of the three security objectives. The security level applies to all information processed by the system. You should review the appropriateness of the potential impact values within the context of the organization, environment, mission, use, and connectivity associated with the system under review.

The general format for expressing the security level, SL, for an information type (as taken from the NIST guidance) is:

SL (information type) = (confidentiality, *impact*); (integrity, *impact*); (availability, *impact*).

where *impact* is Low, Moderate, High, or Not Applicable.

EXAMPLE 1: An information system contains law enforcement information used to investigate bank fraud cases. The investigative information includes the suspect's name, social security number and financial transactions, which require protection under federal law. The disclosure of the contained information could cost the law enforcement agency money and severely damage their reputation and the ability to pursue cases. The loss of the information could impede cases under review. The law enforcement officers can continue to investigate if the information is inaccessible. Therefore, the impact of a loss of confidentiality is severe; the impact of a loss of integrity is severe; the impact of availability is moderate. Management in the organization decides to assign the following potential impact values:

SL (investigative information) = (confidentiality, high); (integrity, high); (availability, moderate).

Note that these assigned weightings are subjective. Mitigation of risk using security controls may reduce the weighting when the system is in production.

When you have determined the security level for each information type handled by the system, then you can determine the overall security level for the information system.

6. Security Level for the Information System

You determine the security level for an information system by combining the potential impact values from the loss of each information type handled by the system. In aggregate, the highest value from among the assigned values for each security objective determines the value for the information system. You determine the system security level by combining the impact levels for each of the three security objectives. Since the values are subjective, you may increase their value or decrease it, when you have mitigated the risk to the information system with additional security controls.

EXAMPLE 2: A bookstore maintains an order-processing system. The order information includes the customer's name and credit card number, which require protection under federal law. The bookstore would suffer severe damage to reputation and to its customers if the order information was disclosed. It would be unable to process the orders and unable to bill the customers if the order information was lost. It would be unable to process new orders if the information was inaccessible, but orders already in-process would still be able to be delivered. Therefore, the impact of a loss of confidentiality is severe, the impact of a loss of integrity is severe, and the impact of a loss of availability is moderate.

The same system also processes the business's tracking information, which is less critical. The tracking information includes the date the order was shipped and its location. There would be little damage if the tracking information was disclosed. The customer would be unable to obtain the status of his order if the tracking information

was lost or inaccessible, but he would still receive his order. Therefore the impact of a loss of confidentiality is low, the impact of a loss of integrity is moderate and the impact of a loss of availability is moderate. Management in the organization decides to assign the following potential impact values:

SL (order information) = (confidentiality, High); (integrity, High); (availability, Moderate).
SL (order tracking information) = (confidentiality, Low); (integrity, Moderate); (availability, Moderate).

The security level for the order-processing system is established by taking the highest values from among the potential impact values assigned to each security objective for each type of information. The resulting security level is:

SL (order-processing system) = (confidentiality, High); (integrity, High); (availability, Moderate).

In Example 2, the information system confidentiality is assigned a value of High, because High is the highest value assigned to any information for that objective. Information system integrity is High because High is the highest value assigned to any information for that objective. Information system availability is Moderate because Moderate is the only value assigned to any information for that objective.

7. References

- Public Law 107-347, **Federal Information Security Management Act of 2002**, December 2002.

- FIPS PUB 199, **Standards for Security Categorization of Federal Information and Information Systems**, December 2003.

- NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, **Volume I**, **Volume II** - Appendix, June 2004.