**Introduction**

This automated approach uses key portions of the Federal Information Processing Standards (FIPS) Publication 199 and National Institute of Standards and Technology (NIST) Special Publication 800-60 to help determine the overall security level of the system being evaluated. The standards and guidelines from FIPS 199 and NIST 800-60 were prepared for use by federal agencies but are applicable to all sectors.

The identification of information processed on an information system is essential to the proper selection of security controls and ensuring the confidentiality, integrity, and availability of the system and its information. Appropriate levels of control will result in information protection that neither overprotects and wastes valuable resources nor under protects placing mission-critical information at risk for compromise.

**Methodology and Definitions**

FIPS 199 assigns impact levels (low, moderate, and high) to the identified security categories (confidentiality, integrity and availability) for both information and information systems. The assigned impact levels are based on the potential impact should certain events occur that jeopardize the information or the systems needed to accomplish the organization’s assigned mission, protect its assets, fulfill its legal responsibilities, maintain day to day operations, and protect individuals.

The three security objectives are defined as:

CONFIDENTIALITY - A loss of confidentiality is the unauthorized disclosure of information.

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

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

The three levels of potential impact are defined as:

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

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

HIGH - 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.

**Process**

There are 3 steps in determining the overall impact level: 1) Identify an information type, 2) Identify system wide factors, and 3) Review and adjust the overall recommended impact level.

1) Identify an Information Type

The first step in this process is to select, from the list provided, one or more types based on the information that is stored, processed, input, or output from the systems under consideration. The selection should be limited to one or more “primary” information types.

As an example, for the information type “Energy Resource Management” the level assignment is:

Confidentiality => Moderate

Integrity => Low

Availability => Low

If more than one type is selected, then the level in each category is the highest of the aggregation. For example if 3 information types are selected and the assignments in the integrity category are low, moderate, high, then the overall assignment for integrity is high.

2) Identify System Wide Factors

The second step is to answer a short set of questions that applies to the information system in general. An affirmative answer to these questions will result in an increase in the security level in one or more categories.

3) Review and Adjust the Overall Recommended Impact Level

This guide will display the overall security assurance level based on the recommended category levels as defined in the NIST SP800-60 and FIPS 199 documents. The highest of the 3 categories is used as the overall system impact level. It is the CSET user’s responsibility to verify the accuracy of the recommendation in light of a complete understanding of the information system and organization. The user can adjust the overall security assurance level to best reflect the unique circumstances associated with the system.

For an accurate determination of the security categorization of the system, a rigorous evaluation should be completed following a comprehensive review of FIPS 199 and NSIT SP800-60.