Data Classification

Security Categorization of Information and Information Systems

Security Categorization of Information and Information Systems

Purpose:

To establish protection profiles and assign control element settings for each category of data for which an Agency is responsible. Security Organization is the basis for identifying an initial baseline set of security controls for the information and information systems.

Security Organization starts with the identification of what information and information systems support which State lines of business, as defined by the Federal Enterprise Architecture (FEA). Subsequent steps focus on the evaluation of the need for confidentiality, integrity, and availability.

Security Categorization of Information and Information Systems

Has anyone in here completed or begun a Security Categorization study for their area?

If you have can you send me a sample of the completed documentation so that OIT can develop consistent format for Collection.

Security Categorization of Information and Information Systems

There are two ISD policy statements pertaining to Security Categorization:

- Standard 500S2-00: Security Categorization of State Information and Information Systems
- Standard 681S1-00: Information Protection

Both these policies will have to be reissued by OIT because they are inconsistent With the NIST guidelines particularly FIPS 199 and SP800-60 Vol 1. which will be the Primary reference utilized in data classification.

Security Categorization of Information and Information Systems

Data Classification Methodology Key References

- FIPS Publication 199, Standards for Security Categorization for Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

- FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems: http//csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

- NIST SP 800-53, Recommended Security Controls for Federal Information Systems Rev.3 http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf

- NIST SP 800-60 Volume 1, Guide for Mapping Types of Information and Information Systems into Security Categories: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

- NIST SP 800-60 Volume 2, Appendices to Guide for Mapping Types of Information and Information Systems into Security Categories: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

Security Categorization of Information and Information Systems

Two Key Definitions

Information Type: *A specific category of information (e.g., privacy, Medical, proprietary, financial, investigative, contactor sensitive Security Management) defined by an organization, or in some Instances, by a specific law, Executive Order, directive, policy or Regulation.*

Information System: *A discrete set of information resources organized for the collection processing, maintenance, use, sharing, dissemination, or disposition of Information.*

Security Categorization of Information and Information Systems

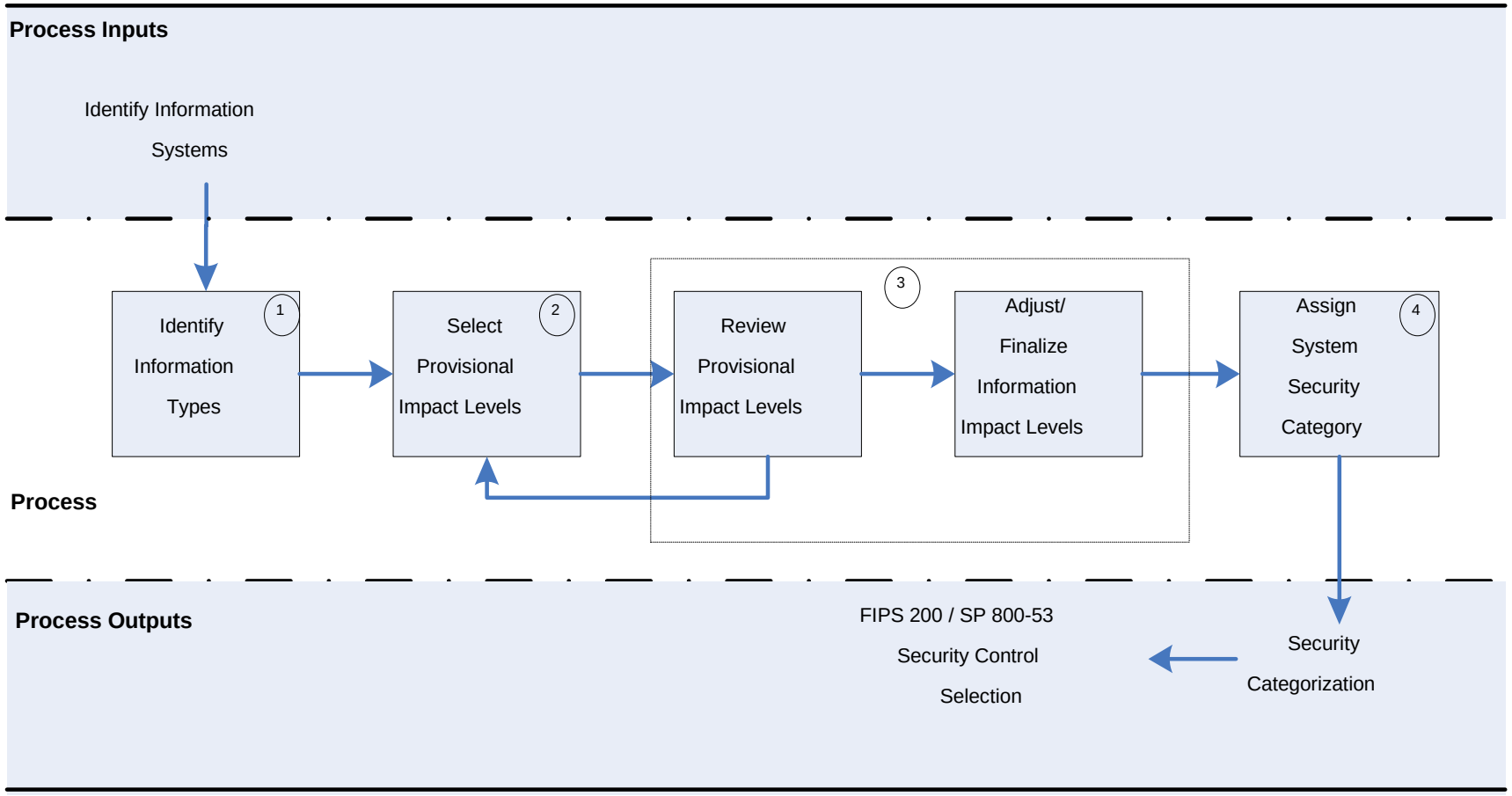

Figure 2: SP 800-60 Security Categorization Process Execution

Security Categorization of Information and Information Systems

An information system supporting the provision of electrical energy to the Data Centre contains the following data types:

a) Detailed electrical energy monitoring information
b) Inventory data related to backup electrical generating, UPS systems and related infrastructure devices

D.7.1 Energy Supply Information Type
Energy Supply involves all activities devoted to ensuring the availability of an adequate supply of energy for the United States and its citizens. Energy Supply includes the sale and transportation of commodity fuels such as coal, oil, natural gas, and radioactive materials. This function also includes distributing and transferring power, electric generation, and/or storage located near the point of use.
;
C.3.4.2 Inventory Control Information Type
Inventory control refers to the tracking of information related to procured assets and resources with regards to quantity, quality, and location..

Information System Name: Power Safe System - DOIT			
Business and Mission Supported: The Power Safe system provides real- time control and information supporting all backup electrical devices supporting the DOIT Data Center.			
Information Types			
Energy Supply	Sensor data monitoring backup power for the DOIT Data Center. This function includes control of distribution and transfer of power. The remote control capabilities can take action such as initiating necessary switching actions to alleviate an overloading power condition. The impacts to this information and the system may affect the installation's critical infrastructures.		
Inventory Control	The Power Safe information system processes routine inventory information on all energy production, storage and monitoring devices.		
Identify Information Types	Confidentiality Impact	Integrity Impact	Availability Impact
Energy Supply	L / L Disclosure of sensor information may impact the Data Center if indications & warnings of overall capability are provided to an unfriendly party.	L / M Significant impacts or consequences may occur if unauthorized modification of information results in incorrect power system regulation or control actions.	L / M Due to loss of availability, severe impact to the DOIT Data Center may result and may in-turn have overall catastrophic consequences for the facility's critical infrastructures.
Inventory Control	L Regardless of the moderate or high impact associated with unauthorized disclosure of some inventory control information, the provisional confidentiality impact level recommended for inventory control information is low.	L The provisional integrity impact level recommended for inventory control information is low.	L The provisional availability impact level recommended for inventory control information is low.
Final System Categorization:	Low	Moderate	Moderate
	Overall Information System Impact: Moderate		

Security Categorization of Information and Information Systems

Overall Goal: To complete the Security Categorization Study for Agencies by end of 2016 Calendar year.

Action Items:

- OIT to rescind and republish any existing policies regarding Security Categorization to be consistent with FIPS 199 &200
- OIT to develop a template for the agencies to record information and information system categorization information
- Agencies to begin the identification of all information systems that impact their mission. Look for system dependencies i.e. Is there any system that is dependent on data from another system or agency.
- OIT to help define Security Categorization Training for agencies and work with agencies to address potential manpower issues.