

Management System: Information Resource Management (IRM)

Subject Area: Cyber Security (and Personally Identifiable Information [PII])

Management System Owner: Ward Best

Point of Contact: Lisa Rawls

Issue Date: 9/4/2012

CBC MS Revision: 0

1.0 Introduction

This subject area describes how the Office of Information Management (IRM) establishes, maintains and monitors cyber security measures sufficient to ensure confidentiality, integrity, and availability of data and systems; and how Controlled Unclassified Information (CUI) is processed and maintained.

The Environmental Management Consolidated Business Center (EMCBC) Cyber Security Program does not mandate what is to be done, but rather stipulates the methods and process to ensure that the final system is secure to within specified parameters.

DOE Order 205.1B provides for the implementation of the Cyber Security Program and sets National Institute of Standards and Technology (NIST) 800-53 as the guiding requirement for all DOE Cyber Security Programs. NIST categorizes the requirements into collections of Management, Operational, and Technical Controls. Each of these Control Areas in turn is broken down into "Families." The Family level provides specific line by line requirements based on the Federal Information Processing Standards (FIPS)-199 security categorization of Low, Medium or High.

ID	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authorization	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management

PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

2.0 Contents

The EMCBC Cyber Security Program is implemented through the use of a system of tiered documents: System Security Plans (PL) and Policy Statements (PS) set the framework performance of the program by providing organizational-specific guidance on implementation, while Information Management Procedures (IMP), Technical Instruction Documents (TID), and Process Instructions describe how the organization will perform the requirements. A Cyber Security Requirements Traceability Matrix is developed to ensure that all requirements have been accounted for and specified for execution in an Implementation Document.

Procedure	Content
1. Cyber Security – System Security Plan for General Support System, PL-240-08	<ul style="list-style-type: none"> Provides the System Security Plan (SSP) for the EMCBC General Support System (GSS) as required by the DOE Cyber Security Management Program – Official Use Only (OUO) Document
2. Policy on the Control of Unclassified Electronic Information, PS-240-06	<ul style="list-style-type: none"> Defines the use and control of all Unclassified Electronic Information at the EMCBC Defines the reporting requirement for loss of control of Controlled Unclassified Information
3. Cyber Security Master Policy, PS-563-01	<ul style="list-style-type: none"> Develops and implements an organizational-wide information security program to safeguard the Information Technology (IT) assets and data
4. Cyber Security – Account Management and User Responsibilities, IP-240-01	<ul style="list-style-type: none"> Establishes the process for managing user accounts, rights, and access to specialized applications Defines user training requirements
5. Cyber Security – Incident Response, IP-240-04	<ul style="list-style-type: none"> Identifies procedures to be followed when an Incident or Potential Incident is identified by users or administrators

Procedure	Content
6. TID 1290-1305*	<ul style="list-style-type: none"> Establishes the process on conducting monthly user account audits
7. TID 1290-1316*	<ul style="list-style-type: none"> Establishes the process for creating two-factor authentication tokens
8. TID 1290-1317*	<ul style="list-style-type: none"> Establishes the process for IT log aggregation and management
9. TID 1290-1320*	<ul style="list-style-type: none"> Establishes the process for maintaining user account control
10. TID 1290-1321*	<ul style="list-style-type: none"> Establishes the process for verifying physical control
11. TID 1290-1323*	<ul style="list-style-type: none"> Establishes the process for maintaining control of Guest Network
12. TID 1290-1325*	<ul style="list-style-type: none"> Establishes the process for conducting incident response testing
13. TID 1290-1326*	<ul style="list-style-type: none"> Establishes the process for the control of stand-alone systems containing sensitive information
14. TID 1290-1328*	<ul style="list-style-type: none"> Establishes the process for controlling network access (SNARE)
15. Procedure 1 – Incident Response (Including Loss of PII)	<ul style="list-style-type: none"> Identifies process to be followed when an incident or potential incident is identified by users or administrators (in development)

* TID documents are considered OOU. Please contact SME for information and access to these documents

3.0 Exhibits/Forms

- [Cyber Security Requirements Traceability Matrix](#)

4.0 Related Information

Information Management Procedures (IMP) constitute a specific group of procedures utilized across the organization for ensuring that cyber security responsibilities that fall outside of the Office of Information Resource Management (IRM) are fully implemented. These procedures

are controlled by IRM. Changes and updates to IMPs are coordinated with affected Offices and Site Offices with the EMCBC.

5.0 Requirements

Document	Title
DOE O 205.1B	Department of Energy Cyber Security Program
PCSP	Department of Energy, Office of the Under Secretary of Energy Program Cyber Security Plan – OOU
OMB M-06-16	Memorandum for the Heads of Departments and Agencies: Protection of Sensitive Agency Information, June 23, 2006
FISMA	Federal Information Security Management Act
HSPD 12	Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors
NIST SP 800-27A	Engineering Principles for Information Technology Security
NIST SP 800-30	Risk Management Guide IT Systems
NIST SP 800-37	Security Certification and Accreditation
NIST SP 800-53	Recommended Security Controls for Federal Information Systems
NIST SP 800-53A	Guide for Assessing the Security Controls in the Federal Information Systems
NIST SP 800-60	Revision 1 – Guide for Mapping Types of Information and Information Systems to Security Categories
FIPS PUB 199	Standards for Security Categorization of Federal Information and Information Systems
DOE O 471.1B	Identification and Protection of Unclassified Controlled Nuclear Information

6.0 Definitions

Term	Definition
Access Approval	Access to information is authorized in writing with justification. Documented approval by a data or system owner to allow user access to information.
Accreditation	Formal declaration by the Designated Approving Authority (DAA) that an information system is accredited to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Accreditation Boundary	The conceptual limit of an information system that extends to all directly and indirectly connected users who receive output from the system without a reliable human review by an appropriately authorized or cleared authority.
Architecture	The configuration of any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; includes computers, ancillary equipment and services, including support services and related resources.
Assistant Director	The Office Director of the specific department that is responsible for the Subject Matter Expert (SME) or Content Owner for a given application.
Assurance	Measure of confidence that the security features, practices, procedures and architecture of an information system accurately mediate and enforce the security policy.
Authority to Operate (ATO)	The system meets the requirements as stated in the System Security Plan.
Certificate & Accreditation (C&A)	All components of a system that are to be accredited by the DAA and excluding separately accredited systems to which the system is connected.
Confidentiality	A security objective that seeks to assure that information is

Term	Definition
	not disclosed to unauthorized persons, processes, or devices. (NSTISSI No. 4009: Assurance that information is not disclosed to unauthorized persons, processes, or devices.)
Consequence of Loss (CoL)	Methodology used to determine the consequence, if any, that might occur if the asset was lost, using the impact factors.
Content Manager	Individual assigned by the Content Owner to manage the development of the application and to ensure the integrity of the data.
Content Owner	The EMCBC Assistant Director responsible for the content and functionality within the given application or system.
Controlled Unclassified Information (CUI)	Unclassified information requiring protection mandated by policy or laws, such as Official Use Only (OUO), Export Control Information (ECI), Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Power Information (NNPI), Personally Identifiable Information (PII), and other information specifically designated as requiring SUI protection such as information identified under Cooperative Research and Development Agreements (CRADA).
Defense-in-depth	Represents the use of multiple computer security techniques to help mitigate the risk of one component of the defense being compromised or circumvented. An example could be anti-virus software installed on individual workstations when there is already virus protection on the firewalls and servers within the same environment. Different security products from multiple vendors may be on different vectors within the network, helping prevent a shortfall in any one defense leading to a wider failure.
Designated Approving Authority (DAA)	Official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.
Domain	A single security boundary of one or more computers that form a computer network.
Electronic Information	Any information stored or transported on electronic media such as hard-drives, flash drives, CDs, DVDs, etc.

Term	Definition
Federal Sponsor	A Federal EMCBC employee who requests specific access to the EMCBC system on behalf of a non-EMCBC user either Federal or contractor.
General Support System	An interconnected set of information resources under the same direct management control that share common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization. [From Office of Management and Budget (OMB) Circular A-130, Appendix III.]
Information System Site Manager (ISSM)	The official responsible for performing the comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent that a particular design and implementation meet a set of specified security requirements, and ensuring the approved security configuration is maintained.
Information Integrity	The preservation of unaltered states as information is transferred through the system and between components.
Information System	The infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information. Any telecommunication or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. [Office of Management and Budget, Circular A-130, Nov. 30, 2000: A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.]

Term	Definition
Information System Security Officer (ISSO)	Person responsible to the system owner and designated approving authority for ensuring the security of an information system throughout its life cycle, from design through disposal. Synonymous with system security officer.
Information Technology (IT)	The hardware, firmware, and software used as part of the information system to perform information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency.
Integrity	Existing when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
Legacy Information System	An operational information system that existed prior to the implementation of the C&A process.
Major Application	A major application is an application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. [From Appendix III, OMB A-130]
Mission	The assigned duties to be performed by an information system.
OIRM	EMCBC Office of Information Resource Management
Offsite User	Users who are not General Access Users under the EMCBC,

Term	Definition
	but require access to specific EMCBC applications in order to coordinate their functions with an EMCBC office. These users are usually at a serviced site or at DOE Headquarters.
Perimeter	All components of an information system that are to be accredited as one entity.
Personally Owned	An item that is owned by an individual and is intended solely for his/her personal use.
Portable Computing Device	Any portable devices that provide the capability to collect, create, process, transmit, store, and disseminate information. They include (but are not limited to) Personal Digital Assistants (PDAs), palm tops, hand-held or portable computers and workstations, non-web-enabled cell phones, web based enhanced cell phones, two-way pagers, and wireless e- mail devices.
Privileged User	A user with access to control, monitoring, or administration functions of the information system (e.g., system administrator, system security officer, maintainers, system programmers, etc.). NOTE: It is often convenient to refer to a user who is NOT a privileged user as a power user.
Protection Profile	An implementation- independent set of security requirements for a category of information systems that meet specific protection measures for specific information groups.
Risk Assessment	Process of analyzing threats to and vulnerabilities of an information system and the potential impact the loss of information or capabilities of a system would have on national security. The resulting analysis is a basis for identifying appropriate and cost-effective countermeasures.
Risk Management	The process concerned with the identification, measurement, control, and minimization of security risks in information systems to a level commensurate with the value of the assets protected.
Security	Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer.

Term	Definition
Security Documentation	All documents which describe the security requirements, design descriptions of security-relevant software and hardware, certification packages, and system security plans. The SSP is the basic system protection document and evidence that the proposed system or major application (or update to either) meets the protection requirements.
Support Personnel	Individuals assigned by the Assistant Director of Information Resource Management (AD-IRM) to control access to the EMCBC domain or other services.
System	The set of interrelated components consisting of mission, environment, and architecture as a whole.
System Administrator	The individual(s) responsible for maintaining and operating the systems and networks within an organization. The System Administrator typically manages user accounts including the deletion, creation, and modification of user privileges. The System Administrators must ensure timely removal of access rights for all departed employees, especially in cases of employee termination.
System Owner	The person ultimately responsible for the overall procurement, development, integration, modification, or operation and maintenance of any given Application, System or Accreditation Boundary. Usually that is the Assistant Director for Information Resource Management.
System Security Plan (SSP)	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
User	Identity of an employee (EMCBC user) or other individual (visitor/non-EMCBC user) having a legitimate business need to access the EMCBC Information System, or other EMCBC services through local network, web or remote access protocols.
User Identifiers	The credentials (user name and password) by which a user identifies himself/herself to the system and by which the system authenticates the user's access.

Term	Definition
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.