

Date 11/19/2015



Environmental Management Consolidated Business Center (EMCBC)

Subject: Configuration Management of Computer Systems and Networks

Information Management Procedure APPROVED:

[Signature]
EMCBC Director

ISSUED BY: Office of Information Resource Management

1.0 PURPOSE

The purpose of this procedure is to define the methods and process to control the configuration of all components that define the cyber security boundary of the Environmental Management Consolidated Business Center (EMCBC) Information Technology (IT) systems.

2.0 SCOPE

This procedure includes all IT functions within the EMCBC and all sites utilizing the EMCBC network systems or managed hardware.

3.0 APPLICABILITY

This procedure is applicable to all IT processes and systems managed by the EMCBC Office of Information Resource Management (IRM). This procedure is not applicable to systems connecting to the EMCBC "hotel type" internet provided for visitors.

4.0 REFERENCES

- 4.1 DOE O 200.1A, Information Technology Management
- 4.2 DOE O 205.1B, Department of Energy Cyber Security Program
- 4.3 EM Risk Management Approach Implementation Plan (RMAIP)
- 4.4 EMCBC PL-240-08 – Cyber Security–System Security Plan for General Support System:
 - 4.4.1 AC-5 Separation of Duties
 - 4.4.2 AC-6 Least Privilege
 - 4.4.3 AC-17 Remote Access
 - 4.4.4 CM-1 Configuration Management Policy and Procedures
 - 4.4.5 CM-2 Baseline Configuration
 - 4.4.6 CM-3 Configuration Change Control
 - 4.4.7 CM-4 Monitoring Configuration Changes
 - 4.4.8 CM-5 Access Restrictions for Change
 - 4.4.9 CM-6 Configuration Setting

- 4.4.10 CM-7 Least Functionality
- 4.4.11 CM-8 Information System Component Inventory
- 4.4.12 CM-9 Configuration Management Plan
- 4.4.13 IA-3 Device Identification and Authentication
- 4.4.14 MA-3 Maintenance Tools
- 4.4.15 MP-4 Media Storage
- 4.4.16 MP-5 Media Transport
- 4.4.17 RA-1 Risk Assessment Policy and Procedures
- 4.4.18 RA-3 Risk Assessment
- 4.4.19 SA-1 System and Services Acquisition Policy and Procedures
- 4.4.20 SA-3 Life-Cycle Support
- 4.4.21 SA-10 Developer Configuration Management
- 4.4.22 SA-11 Developer Security Testing
- 4.4.23 SC-1 System and Communications Protection Policy and Procedures
- 4.4.24 SC-14 Public Access Protections

4.5 PO-IRM-205-10 – Issuing Specialized Information Technology (IT) Equipment

5.0 DEFINITIONS

- 5.1 Configuration Management: The technical and administrative direction and surveillance actions taken to identify and document the functional and physical characteristics of a configuration item; to control changes to a configuration item and its characteristics; and to record and report change processing and implementation status.
- 5.2 Technical Documents: Documents such as safety documents, corrective action dispositions, nonconformance dispositions, contractor progress reports, topical reports, technical papers, functional and operational requirements, design criteria, quality documents and test procedures. Generally technical documents are those containing technical information in the form of data tests results, design criteria, system descriptions, quality functional and operational controls descriptions, and progress/status/action dispositions information, and may include guidance and policy proposals.

6.0 ROLES AND RESPONSIBILITIES

- 6.1 Assistant Director for the Office of Information Resource Management (ADIRM):
The ADIRM has the following responsibilities/duties:
 - Chairs the Configuration Control Board (CCB),
 - Approves Configuration Baseline Changes,
 - Approves Configuration Checklists,
 - Appoints the Member at Large for the purpose of serving on the CCB,
 - Is usually the System Owner,
 - Approves additions to the standard software suite,

- Establishes the minimum scoring levels for the server configurations in accordance with guidance from DOE Headquarters or based on industry standards, and
 - Approves the Network Diagrams.
- 6.2 Cognizant Assistant Director: The EMCBC Office Director of the specific department that is responsible for the content of a given application.
- 6.3 Configuration Control Board: Consists of the ADIRM (Chair), Configuration Control Point Manager and Member at Large. The Configuration Control Board is responsible for reviewing proposed changes and accepting, rejecting, or tabling (placing on hold) the proposed changes based on risk or significant impact to the work processes.
- 6.4 Configuration Control Point Manager (CCPM): The IRM staff member(s) responsible for a particular Configuration Control Point (Desktops, Network, Applications, Appliances and Servers). The CCPM is responsible for managing the configuration of the assigned control point and documenting baseline changes as appropriate.
- 6.5 Content Manager: Individual assigned by the Content Owner to be the point of contact for the development of the application and to ensure the integrity of the data.
- 6.6 Content Owner: The Cognizant Assistant Director or designee responsible for the content and functionality within the given application or system.
- 6.7 IRM Support Personnel: Individuals assigned by the ADIRM to control access to the EMCBC domain or other services. Also responsible for assisting in the completion of all required documentation related to the development and maintenance of applications, EMCBC network systems, and managed hardware.
- 6.8 Information System Security Manager (ISSM): Individual assigned by the ADIRM to ensure adherence to this procedure by the CCPMs.
- 6.9 Information System Security Officer (ISSO): The individual responsible for reviewing logs weekly to ensure that major changes that may affect the security posture have not been made without proper review and for ensuring that noted risks are updated in the Risk Portfolio Manager (RPM) database. The ISSO may designate these responsibilities as needed.
- 6.10 Member at Large: Member of the IRM staff, who is not the CCPM, appointed by the ADIRM for the purpose of serving on the CCB.
- 6.11 System Owner: The lead IRM individual that has overall implementation responsibility for any given application, usually the ADIRM.

- 6.12 Technical Owner / Developer: IRM staff responsible for coding, testing, and placing the application into production, and maintaining the application.

7.0 GENERAL INFORMATION

The configuration management plan is structured to address the different aspects of the many computer systems that make up the EMCBC IT infrastructure. IRM has many diverse elements, from telecommunication devices to servers handling multiple databases. This procedure provides for processes to establish baselines for each of the main configuration areas and then provides for controlled change and expansion of the system to meet the growing IT service area of the EMCBC. The plan provides for methods where security configurations are not defined by specific benchmarks, but where there is technical literature that will support development of secure configurations.

8.0 PROCEDURE

- 8.1 Initial Baselines – Initial Baselines are established at the time of Certification and Accreditation or may be subsequently established as new hardware, software or new applications are added to the system.
- 8.1.1 Development of Initial Baselines - Baselines are developed by the application of DOE standard configurations, as in the case of the DOE Common Operating Environment (DOECO) for desktops, or the use of benchmarks such as the Center for Internet Security (CIS) Security Benchmarks and Defense Information Security Agency (DISA) standards for Servers. If standards or benchmarks do not exist, IRM will develop a baseline configuration based on industry understanding of risks as outlined in trade literature (for example: disabling the use of “magic quotes” in PHP [a hypertext language]). Such in-house baseline checklists will be documented in the form of a Technical Document and will be reviewed periodically to ensure that new risks are addressed and added to the Configuration Control Checklist.
- 8.2 Configuration Management - The EMCBC Configuration Management system is separated into five distinct Configuration Control Points (CCP): Desktops, Servers, Network, Applications and Appliances. Each CCP will be assigned a CCPM. The CCPM is responsible for ensuring the CCP meets the requirements of this procedure.
- 8.2.1 Desktop Configuration – The EMCBC uses a base Operating System installation that is configured using a CIS benchmark tool found at <https://benchmarks.cisecurity.org>. The Operating System is configured per the benchmark tool to meet a minimum score requirement of 80% by applying group policy that is applicable to the default desktop configuration group policy object.
- 8.2.1.1 Laptops – Laptop configurations are developed by manufacturing type. The CIS standards establish laptop configuration.

Microsoft Bitlocker is used to encrypt hard drives on laptops. Users may be allowed limited administrative rights on laptops to facilitate their use off site.

- 8.2.2 Server Configuration – The EMCBC uses CIS benchmarking tools to establish baselines for Server Configurations.
 - 8.2.2.1 Each server will be benchmarked to the appropriate tools based on the function of the server. For example, the public web-server may have a different benchmark score than the web-server used to support the CBC-intranet.
 - 8.2.2.2 Minimum scoring levels will be established by the ADIRM. The scoring levels are derived from guidance from DOE Headquarters and industry standards.

Additional Server Configurations are established based on applications and services the server is hosting. The applications and services include PHP, Microsoft SQL (MSSQL), and Internet Information Services (IIS), etc. This type of software is baselined by using the CIS Benchmark tool and the security checklist and vulnerability scanning methods.
- 8.2.3 Network Configuration – Network configuration is documented by a network diagram(s) showing the interconnections of the network and by documentation of the settings of the security equipment, such as firewalls, router, intrusion detections equipment, etc.
 - 8.2.3.1 Network Diagrams are approved by the ADIRM and the settings on all network appliances are established and approved using the Baseline Configuration Change Form. Note that for clarification, the Voice Over Internet Protocol (VoIP) phones are considered to be a network item (because besides being a phone they are a switch), while the VoIP Server (Media Gateway Controllers) is controlled through server configuration control.
- 8.2.4 Application Configuration (EMCBC) – Application Baselines are established by security checklists and vulnerability scans. These types of checklists establish requirements for coding standards and address issues such as code injection attacks and information control.
 - 8.2.4.1 IRM will maintain a list of the software, the status, and the results of the latest configuration checklist. This requirement only applies to applications developed or modified by changing the code by EMCBC.
- 8.2.5 Appliance Configuration – Appliances are configured on a case-by-case basis. Manufacturer recommendations, industry best practices, and DOE

HQ recommendations are used to configure these devices. Firewalls are configured to deny all and allow by exception. Switches are configured with industry best practices to provide a connection to network resources.

- 8.3 Baseline Configuration Change – Baseline changes are developed and documented on a Configuration Baseline Change Proposal (BCP), IMP-8308-02-F1. Changes to the configuration of a National Security System (NSS) are documented on a Classified Change Proposal (CCP), which uses the same format as IMP-IRM-8308-02-F1. All BCPs are to be completed in SharePoint. Anyone working on a project or application may propose a change. BCPs are initiated from the BCP template in SharePoint and are saved in the BCP folder in the IRM Documents in SharePoint.
- 8.3.1 The proposed change is reviewed by the CCB made up of the ADIRM (Chair), the CCPM, and the Member at Large. Changes may be accepted, rejected, or put on hold pending the need for additional information or the need for off network testing.
 - 8.3.2 The CCB will determine if the system or application needs to be re-baselined by application of the checklist or re-running of a benchmark tool.
 - 8.3.3 The CCB will also determine if there is any residual risk that requires documentation in RPM. The CCPM will be responsible for ensuring that the ISSO updates the risks in RPM.
 - 8.3.4 The CCB will determine if the change will impact the interconnection agreement with DOENet (and thus require completion of HQ CCP form).
 - 8.3.5 The CCB will determine if the change will significantly impact any work process guided by a procedure or plan or other EMCBC document.
 - 8.3.6 All members of the review board will sign the BCP.
 - 8.3.7 All changes made as a result of the BCP will be forwarded to the CCPM. The CCPM will ensure that once activated or installed, all approved Baseline Configuration Changes are documented in the IRM Project Management System.
 - 8.3.8 Each CCPM shall ensure that the Least Functionality in accordance with PP-IRM-240-08, Cyber Security – System Security Plan for General Support System, is being maintained.
- 8.4 Minor Changes – Often during the course of system operations, minor changes need to be made to options or settings of various hardware, software or applications to improve the functionality of the system or applications. These changes may be made by cognizant IRM staff to existing applications in the Configuration Baseline.

8.4.1 These types of changes are to be documented in the IRM Project Management System. The log will be reviewed weekly by the ISSO to ensure that major changes that may affect the security posture have not been made without proper review.

8.4.2 A quarterly review by the Authorizing Official or designee will be conducted to determine if the aggregate effect of the minor changes requires baseline activities.

8.5 IRM Project Management System - All actions such as changes, reviews, and audits associated with the EMCBC Information Systems are documented in the IRM Project Management System. Items that change configurations are indicated as such in the log/ticket.

9.0 RECORDS MAINTENANCE

Records generated through implementation of this procedure are identified as follows and are maintained by IRM in accordance with the EMCBC Organizational File Plan:

Records Category Code	Records Title	Responsible Organization	Quality Records Classification (Lifetime or Non-Permanent)
DAA-GRS-2013-0005-0007	System Development Records	OIRM	N/A
DAA-GRS-2013-0005-0004	Information Technology Operations and Maintenance Records	OIRM	N/A

9.1 References – Forms/Attachments/Exhibits

9.1.2 Forms

IMP-IRM-8308-02-F1, Configuration Baseline Change Proposal (BCP) Template (actual form maintained in SharePoint)

CM Information Resource Management EMCBC	Baseline Change Proposal	Control Point: Choose a control point.
	Title: Click here to enter text.	Requested By: Click here to enter text. Date: Click here to enter date requested.
	Number: Click here to enter text.	
Proposed Change: Click here to enter change.		
Additional Testing or Baseline Testing required? Choose an item. Does this Change affect Interconnect with DOENet? Choose an item. Does this Change significantly affect any documents, procedures, plans? Choose an item.		
Impacted Systems and Applications: Click here to enter impacted systems and applications.		
Status: Approved		
Control Point Manager: X _____ Click here to assign Control Point Manager.		
Member at Large: X _____ Click here to assign Member at Large.		
Assistant Director for IRM: X _____		
ADIRM Approval		

EMCBC RECORD OF REVISION**DOCUMENT - Configuration Management of Computer Systems and Networks**

If there are changes to the controlled document before the two-year review cycle, the revision number stays the same; one of the following will indicate the change:

I Placing a vertical black line in the left margin adjacent to sentence or paragraph that was revised; or

I Placing the words GENERAL REVISION at the beginning of the text. This statement is used when entire sections of the document are revised.

If changes and updates occur at the two-year review cycle, the revision number increases by one.

Rev. No.	Description of Changes	Revision on Pages	Date
0	Initial Information Management Procedure Supersedes IP-240-02, Rev. 2 dated 6/14/10	Entire Document	9/28/12
1	Periodic Review		11/19/15
	Completing Baseline Configuration		
	Change documents	6	
	Changed document title PL-240-08 to PP-IRM-240-08	6	
	Removed Attachment A (same as form)	7	