

No: Y15-406INS

Title: *Information Technology Configuration Management Instruction*

Rev: 04/04/02

This instruction conveys the process for managing the configuration of information technology components at the Y-12 National Security Complex in Oak Ridge, Tennessee.

A hard copy of this document is valid only until the document revision date has changed on the Web. The hard copy should be dated and signed the day it is printed. If you continue working from the hard copy, you should verify its accuracy on the Web.

Date Printed: _____

Verifier: _____

**BWXT Y-12, L.L.C.
Management Requirements**

Number: Y15-406INS
Rev. Date: 04/04/02
Supersedes: Y15-106
Page: 1 of 24

BWXT Y-12
Management Control

Subject: Information Technology Configuration Management Instruction

Paul M. Parris /s/
Instruction written by

04/05/02
Date

Approvals: [Approval Signatures and Dates on File]

W. D. Beard /s/
Functional Area Manager/Owner

04/05/02
Date

George A. Dailey /s/
Functional Area Manager/Owner

04/08/02
Date

Doris Heim /s/
Executive Manager

04/10/02
Date

M. J. Keyser /s/
Requirements and Issues Management

04/22/02
Date

06/01/02
Effective Date

Re-Affirm Date

This document has been reviewed by an Authorized Derivative Classifier and UCNI Reviewing Official and has been determined to be UNCLASSIFIED and contains no UCNI. This review does not constitute clearance for public release.

D. O. Colclasure /s/ 04/05/02
Signature and Date

Subject: Information Technology Configuration Management Instruction

CONTENTS

1. INTRODUCTION.....	4
1.1 Purpose.....	4
1.2 Scope.....	4
1.3 Other Documents Needed.....	5
2. PROGRAM STRATEGY AND IMPLEMENTATION	5
2.1 Introduction.....	5
2.2 Programmatic Implementation Responsibilities	5
2.2.1 Roles and Responsibilities	5
2.2.2 Emergency Changes.....	7
2.2.3 Standard Configurations.....	8
2.3 Network-Connected Server Hardware and Associated Software	9
2.3.1 Background on Responsibilities	9
2.3.2 Roles and Responsibilities	9
2.4 Network-Connected Printers.....	12
2.4.1 Background on Responsibilities	12
2.4.2 Roles and Responsibilities	12
2.5 Software	14
2.6. Network Infrastructure Hardware and Software.....	14
2.6.1 Background on Responsibilities	14
2.6.2 Roles and Responsibilities	15
2.7 World Wide Web Content	16
2.7.1 Background on Responsibilities	16
2.7.2 Roles and Responsibilities	16
2.8 Personal Computing and Other Network-Connected Computing Devices, Associated Software, and Peripherals.....	19
2.8.1 Background on Responsibilities	19
2.8.2 Roles and Responsibilities	19
3. SOURCE DOCUMENTS.....	21
4. RECORDS.....	22
APPENDIX A	
Acronyms and Definitions.....	23

Subject: Information Technology Configuration Management Instruction

REVISION LOG

(Page 1 of 1)

Revision Date	Description of Change	Pages Affected
04/04/02	This is a new instruction. It supersedes Y15-106, <i>Internet Servers and Web Information Release</i> . It has been prepared in response to issues raised during the October 2001 Inspection and Evaluation at the Y-12 National Security Complex in Oak Ridge, Tennessee. DMR 02-15/406-001 has been completed to initiate this revision.	All

Subject: Information Technology Configuration Management Instruction
--

1. INTRODUCTION

1.1 Purpose

This instruction conveys the process of managing the configuration of information technology (IT) components at the Y-12 National Security Complex (Y-12) in Oak Ridge, Tennessee.

Configuration management, carried out in a manner that ensures overall quality and security, is a key part of work performance at Y-12. Configuration management ensures, for the lifetime of a component, systems are installed and managed consistently, changes are approved properly, a change history is maintained for defined cases, and periodic audits are performed.

1.2 Scope

This instruction applies to all instances of the following components at Y-12 [where “network-connected” means connected to the network at any time, as indicated by assignment of a Y-12 network Internet Protocol (IP) address]:

- network-connected server hardware and associated software;
- network-connected printers;
- application software, including commercial-off-the-shelf, operating on network-connected server hardware;
- network infrastructure hardware and software;
- World Wide Web content, including information release; and
- personal computers and other network-connected computing devices, associated software, and peripherals.

This instruction applies to components operating at any security classification level at Y-12, including unclassified, unclassified national security related (UNSR), and classified. Taken as a whole, the previously mentioned components comprise the network-connected hardware, software, and manufacturing and office-computing infrastructure for Y-12. This infrastructure is essential to the performance of various work activities at Y-12, whether business- or manufacturing-related. The IT Configuration Management Program defines requirements for all these components to ensure security and quality requirements for Y-12 are followed consistently and effectively.

This instruction also applies to other contractors/tenants and subcontractors at Y-12, as communicated through their contractual agreements.

The responsibilities in this instruction apply for the entire life cycle of a given IT component at Y-12, regardless of the Y-12 owner of that component.

This instruction does not apply to the following, although it may be followed as a best business practice, as appropriate:

- embedded firmware contained in commercially procured office or lab devices (e.g., microwave ovens, telephones, hand-held devices or instruments);

Subject: Information Technology Configuration Management Instruction
--

1. INTRODUCTION (CONT.)

1.2 Scope (cont.)

- programmable logic controllers, machine controllers, and similar devices, unless connected to a Y-12 network; and
- hardware and software that never are connected to a Y-12 network.

1.3 Other Documents Needed

- UCN-7721B, "Y-12 Information Control"
- UCN-20295, "Information Server Registration"
- UCN-20297, "Approval for Web Site Information"
- Y15-405PD, *Information Technology Configuration Management Program*
- Y15-902, *Management Assessment*
- Y15-903, *Independent Assessment*
- Y19-203INS, *Manual for the Protection and Control of Classified Matter and Other Protected Information*
- Y60-101PD, *Quality Program Description*
- Y80-101INS, *Software Management Instruction*

2. PROGRAM STRATEGY AND IMPLEMENTATION

2.1 Introduction

The information provided herein on IT configuration management applies to all network-connected items at Y-12. Each IT component area covered by this instruction is represented in the following sections. For each area, pertinent background information is provided as necessary. Following that, specific roles and responsibilities for each area are provided, in no prescribed order. The individual or organization listed is responsible for performing the activities shown for the life cycle of a given IT component, unless the individual or organization delegates the activities, in writing, to another party.

2.2 Programmatic Implementation Responsibilities

There are certain responsibilities and activities within the scope of IT configuration management that cut across all subject areas covered by this instruction. These responsibilities and activities, and the organizations charged with performing related tasks, are detailed in Section 2.2.1.

2.2.1 Roles and Responsibilities

Information Systems and Technology (IST)

- Defines the IT Configuration Management System (IT-CMS) and its parameters and provides for the system's availability and maintenance.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.2 Programmatic Implementation Responsibilities (cont.)

2.2.2 Roles and Responsibilities (cont.)

IST (cont.)

- Leads performance of a yearly, random audit of configuration management components and areas covered by this instruction. These audits may be performed as management or independent assessments as defined in Y15-902, *Management Assessment*, and Y15-903, *Independent Assessment*.
- Updates this instruction and Y15-405PD, *Information Technology Configuration Management Program*, as necessitated by changes in Y-12 contract requirements and business rules and U.S. Department of Energy (DOE)/National Nuclear Security Administration (NNSA) requirements.
- Leads preparation and ongoing updates of implementing guidance for components and areas covered by this instruction. This implementing guidance can be found on the Y-12 internal Web server at the IST organization's home page.
- Provides guidance regarding the Y-12 IT Configuration Management Program and approves specific supporting systems, tools, and other technologies.
- Communicates across Y-12 any changes in IT configuration management requirements.

Computing and Telecommunications Security Organization (CTSO)

- Defines security policies for IT components. Security requirements are contained in Y19-401INS, *Automated Information System (AIS) Security Handbook*.
- Provides DOE/NNSA security guidance that affects IT configuration management and manages its incorporation into the program.
- Leads or participates in a yearly, random audit of configuration management components and areas covered by this instruction. These audits may be performed as management or independent assessments as defined in Y15-902, Y15-903, and Y19-401INS, Chapter 13.
- Communicates across Y-12 any changes in security requirements that impact configuration management.
- Defines security-related testing and validation criteria for configuration changes.

Quality Assurance

- Defines applicable Y-12 Quality Program requirements contained in Y60-101PD, *Quality Program Description*, and supports incorporation of these requirements into the IT Configuration Management Program.
- Supports proper implementation of quality assurance requirements.

Maintenance Support

- Modifies components managed within the program and complies with proper approvals and program guidance.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.2 Programmatic Implementation Responsibilities (cont.)

2.2.2 Emergency Changes

2.2.2.1 Background on Emergency Changes

Certain changes to components managed as part of the IT Configuration Management Program periodically may require immediate modifications for security or other reasons. After completion of an authorized emergency change, all requirements within this instruction must be met, as described below. The requirements in Section 2.2.2.2 describe the method of implementing emergency changes within the program.

2.2.2.2 Roles and Responsibilities

System Owner (SO)

- Requests and authorizes an emergency change to components for which he or she is responsible. Emergency changes must be authorized in written form, which may include e-mail.
- Consults CTSO before authorizing a security-significant emergency change.
- Initiates, within five working days of the emergency change, the process to fully comply with all requirements contained in this instruction.
- Defines testing criteria for business- and technical-related emergency changes, including conformance to security testing requirements.

Information Owner (IO)

- Requests and authorizes an emergency change to components for which he or she is responsible. Emergency changes must be authorized in written form, which may include e-mail.
- Consults CTSO and the Classification and Technical Information Office (C/TIO) before authorizing a security-significant emergency change.
- Initiates, within five working days of the emergency change, the process to fully comply with all requirements contained in this instruction.

CTSO

- Approves security-significant emergency changes.

C/TIO

- Approves security-significant emergency changes to World Wide Web content.

System Manager/Administrator (SMA)

- Implements and tests approved emergency changes.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.2 Programmatic Implementation Responsibilities (cont.)

2.2.2 Emergency Changes (cont.)

Information Maintainer (IM)

- Implements approved emergency changes.

2.2.3 Standard Configurations

2.2.3.1 Background on Standard Configurations

There will be two forms of standard configurations requirements under the IT Configuration Management Program. The first form relates to security and requires conformance with Y19-401INS and Master Security Plan requirements as detailed on the CTSO Web site. The second form of standard configuration relates to business and technical standards. These configurations will be prepared by IST and published on the IST Web site. Technical support tools may be supplied to enable compliance with these configurations. In selected cases, as approved by IST and CTSO, deviations from these standards will be permitted where compliance would result in a negative impact on the ability to perform Y-12-related work. For approved deviations, all other requirements within this instruction shall apply. Standard business and technical configurations shall be supplied only for selected IT elements, as designated by IST.

2.2.3.2 Roles and Responsibilities

SO

- Consults CTSO before requesting security-significant deviations from standard configuration requirements.
- Requests from IST any deviations from standard configuration requirements for components for which he or she is responsible.

CTSO

- Defines standard security configuration requirements for IT components.
- Defines security testing criteria for standard configuration changes and deviations from standard configurations.
- Approves requests for security-significant deviations from standard configurations.

SMA

- Implements and tests approved deviations from standard configuration requirements.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.2 Programmatic Implementation Responsibilities (cont.)

2.2.3 Standard Configurations (cont.)

IST

- Defines standard technical and business configuration requirements for IT components.
- Defines business and technical testing criteria for standard configurations and deviations from standard configurations.
- Designates IT components that must conform to standard technical and business configuration requirements.
- Approves requests for deviations from standard configurations.

2.3 Network-Connected Server Hardware and Associated Software

2.3.1 Background on Responsibilities

Section 2.3.2 of this instruction defines the process by which the configuration of Y-12 server computers and associated systems software will be managed. This process governs configuration management for all server computers for which BWXT Y-12, L.L.C. (BWXT Y-12) has managerial responsibility and that are connected to a Y-12 network at any time.

BWXT Y-12 manages several hundred server computers spanning multiple hardware and operating system software types from many different vendors. These server computers provide various services (e.g., database, Web, e-mail, application development, application hosting, networking, file) in support of practically every business function performed at Y-12. There is, therefore, a large amount of systems software, or layered products, installed on these servers. This software includes database management systems (e.g., Oracle®, SQL Server); Web servers (e.g., Apache, Internet Information Server); and application development tools (e.g., C/C++™, Java™, Macromedia® ColdFusion®).

The multitude of combinations of hardware, operating systems, systems software/layered products, applications, and application development tools comprises a large number of configurations that must be managed to achieve the level of security, safety, and operational efficiency required at Y-12.

The IT-CMS defines the baseline for configuration management of Y-12 servers. IST creates the IT-CMS and ensures maintenance of relevant data about Y-12 servers that are connected to the Y-12 network at any time and their respective configurations.

2.3.2 Roles and Responsibilities

SO

- Performs business oversight of the network-connected server on an ongoing basis. This includes providing subject-matter expertise related to the server's function.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.3 Network-Connected Server Hardware and Associated Software (cont.)

SO (cont.)

- Serves as the primary point of contact for compliance with IT configuration management requirements.
- Reviews the IT-CMS annually, at a minimum, to verify the accuracy of the data for servers for which he or she is responsible.
- Enters into the IT-CMS all required data about any existing server or planned new server.
 - If a new server is to be acquired via purchase requisition or redeployment, the SO enters into the IT-CMS all required data about the new or redeployed server. This information must be entered within ten working days of the input date of the requisition or the date of the redeployment decision.
 - If a change is required for an existing server, the SO enters into the IT-CMS all required data about that server. This information must be entered within ten working days of the date the SO initiates the change.
- Obtains server configuration approvals from the information system security officer (ISSO) and CTSO for the following:
 - the proposed configuration of any new server;
 - proposed changes to the configuration of existing classified and UNSR servers; and
 - proposed, security-significant changes to the configuration of unclassified servers.
- Prepares and maintains a record in the IT-CMS of any server changes, additions, or deletions. The record shall contain, at a minimum,
 - identification (ID) of the server,
 - ID of the server change,
 - date of the server change,
 - description of the server change,
 - ID of the server change requester,
 - ID of the technical approver,
 - ID of the administrative approver,
 - ID of the server change implementer,
 - ID of the ISSO approver (if applicable),
 - ID of the CTSO approver (if applicable), and
 - ID of the server change tester (if applicable).
- Works with the appropriate SMA to define and implement a secure server configuration for new servers or for security-significant changes to existing servers.
- Provides an approved Information System Security Plan (ISSP) regarding system configuration and security profile for classified and UNSR systems or unclassified systems, as designated by CTSO.
- Defines testing criteria for business- and technical-related configuration changes, including conformance to security testing requirements.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.3 Network-Connected Server Hardware and Associated Software (cont.)

SMA

- Maintains the network-connected server in proper working order. This maintenance includes software installation, system configuration, and resource usage monitoring.
- Works with the SO, ISSO, and CTSO to define, propose, and implement secure configurations for new servers. Security requirements are contained in Y19-401INS.
- Works with the SO, ISSO, and CTSO to define and implement secure configurations if a change is proposed for an existing classified or UNSR server.
- Determines whether a planned change to the configuration of an existing unclassified server has security ramifications. If the change is determined to have security ramifications, the SMA works with the SO and CTSO to define and implement secure configurations.
- Registers information servers with CTSO by completing UCN-20295, "Information Server Registration."
- Tests configuration changes.
- Provides input to the ISSP regarding system configuration and security profile of classified and UNSR systems or unclassified systems, as designated by CTSO.

IST

- Creates and maintains the IT-CMS.
- Communicates annually with all SOs of record to require a review of the IT-CMS. The purpose of this review by the SO is to verify the accuracy of the data for those servers for which he or she is the designated SO.

CTSO

- Works with the SO and SMA to define proposed server configurations.
- Reviews and approves or denies proposed server configurations.
- Reviews and approves or denies the ISSP for classified, UNSR, or other systems, as specifically designated by CTSO.

ISSO

- Works with the SO and SMA to define proposed server configurations.
- Reviews and approves or denies proposed server configurations.
- Prepares, reviews, and approves or denies the ISSP for classified and UNSR systems or other systems, as specifically designated by CTSO.

Information System Security Site Manager (ISSM)

- Reviews and approves or denies the ISSP for classified and UNSR systems.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.4 Network-Connected Printers

2.4.1 Background on Responsibilities

Section 2.4.2 defines the process used to manage the configuration of Y-12 network printers. The responsibilities listed in this section apply to all network printers for which BWXT Y-12 has managerial oversight and that are connected to the Y-12 network at any time.

BWXT Y-12 manages several hundred networked printers, primarily in the unclassified environment. The IT-CMS defines the baseline for configuration management of network printers. IST creates the IT-CMS and sets requirements for the entry and maintenance of data related to network printers.

2.4.2 Roles and Responsibilities

SO

- Serves as the responsible party on an ongoing basis for the business use of the network printer.
- Serves as the primary point of contact for compliance with IT configuration management requirements.
- Registers in the IT-CMS the following network configuration parameters for each printer:
 - IP name and address;
 - classification level of printed data;
 - ID of SMA and SO;
 - descriptive characteristics of printer (e.g., manufacturer, model);
 - type of network device (set to “Network Attached Printer”);
 - ID of printer;
 - location of printer, including site, building, and room; and
 - address of Network Interface Card (NIC).
- Defines and maintains an access control list for printers for which he or she is responsible.
- Updates data in the IT-CMS as changes occur to printers for which he or she is responsible. Changes must be entered into the IT-CMS within ten working days of completion.
- Reviews and updates annually, at a minimum, information in the IT-CMS for each printer for which he or she is responsible.
- Enters into the IT-CMS all required data about any existing printer or planned new printers.
 - If a new printer is to be acquired via purchase requisition or redeployment, the SO enters into the IT-CMS all required data about the new or redeployed printer. This information must be entered within ten working days of the input date of the requisition or the date of the redeployment decision.
 - If a change is required for an existing printer, the SO enters into the IT-CMS all required data about that printer. This information must be entered within ten working days of the date the SO initiates the change.
- Provides an approved ISSP regarding system configuration and security profile for classified and UNSR network printers or unclassified printers, as designated by CTSO.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.4 Network-Connected Printers (cont.)

SO (cont.)

- Defines testing criteria for business- and technical-related configuration changes, including conformance to security testing requirements.

SMA

- Maintains the network-connected printer in proper working order. This maintenance includes system configuration.
- Implements and maintains the security settings for all network printers. The SMA may delegate implementation of the security settings to the Computer Helpline. Required security settings can be found on the internal Web server at the IST organization's home page.
- Configures network-connected printers in accordance with guidance provided on the internal Web server at the IST organization's home page.
- Implements a printer access control list, as defined by the SO.
- Provides input to the ISSP regarding system configuration and security profile for classified and UNSR network printers or unclassified network printers, as designated by CTSO.
- Implements print queues via centrally supported network print servers.
- Tests configuration changes.

IST

- Defines network printer configuration requirements, including management requirements.
- Communicates annually with SOs of record to require a review of the IT-CMS. The purpose of this review by the SO is to verify the accuracy of the data for those network printers for which he or she is the designated SO.

CTSO

- Reviews and approves or denies the ISSP for classified, UNSR, or other printers, as specifically designated by CTSO.
- Works with the SO and SMA to define proposed configurations for classified and UNSR network printers.
- Reviews and approves or denies proposed configurations for classified and UNSR network printers.
- Defines network printer security requirements. Security requirements are contained in Y19-401INS.

ISSO

- Prepares, reviews, and approves or denies the ISSP for classified, UNSR, or other printers, as specifically designated by CTSO.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.4 Network-Connected Printers (cont.)

ISSO (cont.)

- Works with the SO and SMA to define proposed configurations for classified and UNSR network printers.
- Reviews and approves or denies proposed configurations for classified and UNSR network printers.

ISSM

- Reviews and approves or denies the ISSP for classified and UNSR systems.

2.5 Software

Y80-101INS, *Software Management Instruction*, implements configuration management requirements for application software.

2.6 Network Infrastructure Hardware and Software

2.6.1 Background on Responsibilities

Section 2.6.2 of this instruction defines the process by which the configuration of Y-12 networking software and hardware will be managed. This process governs configuration management for networking components on the Y-12 data communications networks, including both the Unclassified Services Network and the Classified Services Network for which BWXT Y-12 has managerial responsibility.

Networking hardware components consist of routers, bridges, switches, concentrators, hubs, firewalls, modems, specialized network servers, and the various types of networking media (e.g., coaxial, fiber optics, twisted-pair), including point-to-point circuits, both on- and offsite. Networking software consists of the operating systems (e.g., Cisco IOS) for the manageable devices previously mentioned and specialized applications running on standard servers (e.g., Domain Name Service, HP Open View, Cisco Works).

Configuration management and change controls for the Y-12 networks are accomplished using several methods. Databases for each network contain information relating to each IT device that is connected to the network. These databases are required for the technical operation of each network. The information they contain includes device hardware addresses, assigned IP addresses, owner ID, location, and connectivity. Databases also are maintained to track the paths and endpoints for network media and point-to-point circuits. Network drawings provide a mapping of the networking devices in use to the building level on each network. Engineering drawings provide detailed information of intrabuilding media layouts and interbuilding cabling links. Software configuration of the manageable networking components is controlled by record-keeping methods established for each network within the IT-CMS.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.6 Network Infrastructure Hardware and Software (cont.)

The responsibilities in Section 2.6.2 do not apply to configuration management of IT devices such as computer hosts, front-end processors, desktop systems, or servers that are not used exclusively for network management or control. Configuration management roles and responsibilities for IT components used for purposes beyond network management or control are covered in the other sections of this instruction.

2.6.2 Roles and Responsibilities

SO

- Registers with the Network Management Center all devices that access the Y-12 network.
- Updates device registration information when moves, additions, or changes are made.

Network Managers (i.e., IST)

- Maintain standard configuration guidelines for each type of networking device.
- Approve configuration changes that alter the system baseline.
- Monitor execution of the configuration management plan.
- Maintain baseline and configuration-related documentation for managed network components.

CTSO

- Approves configuration changes per NNSA and Y-12 requirements.
- Approves baseline configuration settings for networking components.
- Advises IST network managers of required security posture and extant security patches relating to networking devices used on the networks.

Engineering and Technology

- Maintains engineering drawings pertaining to the networks.
- Incorporates configuration management requirements in network designs.

Networking Services Provider

- Maintains accuracy of databases for network devices and media/circuits.
- Provides proper documentation of configuration changes.
- Maintains network drawings to reflect the connectivity of networking components and media comprising the network.
- Implements configuration changes after obtaining required approvals.
- Maintains documentation of configurations for networking components.
- Labels networking components properly.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.7 World Wide Web Content

2.7.1 Background on Responsibilities

Section 2.7.2 defines the process, approvals, and controls necessary for placing and maintaining information on all Web servers managed or controlled by BWXT Y-12. The responsibilities listed in this section apply to all information areas on Web servers managed or controlled by Y-12 personnel. They do not apply to Web-based applications, which are covered in Section 2.5 of this instruction.

Y-12 manages several hundred information areas in various formats in three environments—internal, external, and classified. There is growing demand for Web services in the Unclassified Controlled Nuclear Information (UCNI) environment, but there currently is no centralized infrastructure in place.

2.7.2 Roles and Responsibilities

This section lists general responsibilities related to World Wide Web content management at Y-12.

IO

- Provides business oversight of a Web-based information area on an ongoing basis. This includes providing subject-matter expertise related to the information area.
- Contacts Communications Services for requirements for setting up Web pages or Web sites and information on guidelines and standards.
- Determines the information's intended audience and the appropriate server (i.e., external, internal, UCNI, or classified), based on the information's classification level, sensitivity, level of access control, and location and the intended audience's Web-access tools.
- Obtains review and approval of all initial site content from an authorized derivative classifier and Communications Services, and from C/TIO, as appropriate, for
 - the proposed addition of any new information area;
 - proposed changes to classified and UNSR information on classified and UNSR servers; and
 - proposed, security-significant changes to the content of information on unclassified servers

before placing the content on a Web server. UCN-20297, "Approval for Web Site Information," must be completed as part of the review and approval process. This form can be found on the Y-12 home page under Just-In-Time Forms.

- Registers an information area on the appropriate server by submitting a copy of the approved UCN-20297 to IST.
- Assigns Need-to-Know requirements to all Web pages.
- Reviews Web information at required intervals, or more frequently as necessary, to confirm it is correct and business-related and adheres to all security and C/TIO requirements.
- Ensures links to external sites (i.e., sites outside the y12.doe.gov domain) are business-related.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.7 World Wide Web Content (cont.)

IO (cont.)

- Ensures information remains current. The IO also secures site-maintenance funding and identifies primary and alternate maintainers.
- Ensures Web site contents do not obligate anyone without his or her knowledge.
- Verifies a link to the security notice appears on the home page of all internal Web sites and on all external Web pages.
- Coordinates proper handling of copyright implications for Web site contents. When copyrighted information created by an outside entity is included, the IO obtains written permission from the copyright holder and verifies the material is properly cited. The IO identifies trademarks with the trademark symbol (i.e., ® or ™).
- Verifies BWXT Y-12 logos, as well as navigation and other required links, conform to the common user interface standards developed by Y-12 Communications Services.

SMA

- Manages the Web server per requirements as defined in this instruction and by Y-12 security requirements.
- Adds and removes information areas.
- Maintains registration information.
- Manages the search engine according to IST direction.
- Manages Web server products according to IST direction.

IM

- Certifies that proper approvals have been obtained, records are on file, and updates to the information area reflect decisions of C/TIO and Communications Services regarding reapproval.
- Contacts IST for architectural requirements for Web software.
- Validates proper operation of security features.
- Authorizes publication of the information on the Web server after all requirements have been satisfied.
- Informs the appropriate IST personnel when the IO changes.
- Confirms no Web page or application sends clear text passwords across the network.
- Verifies Web servers and databases for classified systems do not reside on the same physical server, unless approved by the ISSM.
- Includes a reminder on all sites that all printed pages be handled according to Y19-203INS, *Manual for the Protection and Control of Classified Matter and Other Protected Information*.
- Adds files to an information area.
- Configures and documents Need-to-Know controls on all resources accessed through Web sites.
- Performs the following tasks:
 - removes all files from the Web server when an information area no longer is needed,

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.7 World Wide Web Content (cont.)

IM (cont.)

- updates the registration with IST to reflect that the information area no longer is active, and
- notifies via e-mail the SMA or the SMA's delegate when an information area no longer is needed and requests that the area be removed from the Web server.

IST

- Provides Web infrastructure to meet business needs.
- Approves any technology changes.
- Sets strategic direction for Web technology and use.
- Sets requirements for servers, domain names, network connections, and security. Security requirements are contained in Y19-401INS.
- Verifies all external Web servers are attached to the Y-12 Data Management Zone.
- Verifies all Web sites and servers are referenced appropriately in the Y-12 government domain.
- Ensures all external Web sites are located on the centrally managed external Web servers.
- Oversees compliance of all Web servers with this instruction and all Y-12 security requirements.
- Provides architectural requirements to which all Web infrastructure and projects must adhere.

IST and CTSO

- Review servers and information areas to confirm compliance with Y-12 requirements.

Communications Services

- Leads efforts to identify, develop, and configure essential Web content for Y-12.
- Provides central coordination for development of internal and external Web pages and sites, interfacing with IST, Y-12 Public Relations, external vendors, and others as needed.
- Provides initial needs assessment and guidance on setting up Web pages or sites on internal or external servers.
- Establishes design, content, and usability standards for Y-12 Web pages and sites.
- Reviews content of submitted Web pages or sites for compliance with requirements, instructions, and standards.
- Initiates a twice-yearly review of all information on Web servers for compliance with Y-12 requirements and federal usability standards and guidelines related to Web sites.
- Works with IOs and IMs to support appropriate maintenance of site contents.
- Verifies C/TIO's approval of initial content and subsequent content changes.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.7 World Wide Web Content (cont.)

C/TIO

- Reviews both initial content and subsequent changes or additions to an information area. Classification provides final reviews for classification and UCNI; Technical Information reviews for Privacy Act, Copyright Act, Export Control, and other unclassified sensitive information.
- Completes appropriate sections of UCN-20297 for initial reviews of an information area.
- Completes appropriate sections of UCN-7721B, "Y-12 Information Control," for reviews of changes or additions to information area content, if indicated per the initial information area review, as documented on UCN-20297. Changes or additions that are solely editorial and/or nonsubstantive in nature do not require a C/TIO review. If a hard copy of the information has been previously reviewed and cleared for public release, C/TIO approval is not required. (To obtain a copy of the appropriate UCN-7721B for such a document, contact C/TIO.)

2.8 Personal Computing and Other Network-Connected Computing Devices, Associated Software, and Peripherals

2.8.1 Background on Responsibilities

Section 2.8.2 defines the process used to manage the configuration of Y-12 desktop computing devices and associated hardware and software. This process governs configuration management for all desktop computing devices for which BWXT Y-12 has managerial responsibility and that are connected to the Y-12 network.

BWXT Y-12 manages more than 4000 desktop computing devices. A computing device based on a Microsoft® operating system is the preferred type. The IT-CMS defines the baseline for configuration management of desktop computing devices. IST creates the IT-CMS and sets requirements for the entry and maintenance of data related to network-connected desktop computing devices.

2.8.2 Roles and Responsibilities

SO

- Serves as the responsible party on an ongoing basis for the business use of the personal computing device. This usually is the primary user of the device.
- Serves as the primary point of contact for compliance with IT configuration management requirements.
- Maintains a software inventory to demonstrate compliance with licensing of desktop products, per IST requirements. The requirements are located on the internal Web server at the IST organization's home page.
- Notifies the SMA of any software and/or hardware products added to or removed from a desktop computing device assigned to him or her in the IT-CMS.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.8 Personal Computing and Other Network-Connected Computing Devices, Associated Software, and Peripherals (cont.)

SO (cont.)

- Provides an approved ISSP regarding system configuration and security profile for classified and UNSR systems or unclassified systems, as designated by CTSO.
- Defines testing criteria for business- and technical-related configuration changes, including conformance to security testing requirements.

SMA

- Maintains the personal computing device in proper working order. This maintenance includes system configuration. The SMA and the SO may be the same person, but this is not required (e.g., one SMA may administer a group of personal computing devices).
- Implements and maintains the required security settings for all desktop computing devices, including share points (e.g., folders) and input/output devices. Required security settings can be found on the internal Web server at the IST organization's home page.
- Tests configuration changes.
- Enters into the IT-CMS all required data about any existing personal computer, network-connected computing device, or planned device.
 - If a new personal computer or network-connected computing device is to be acquired via purchase requisition or redeployment, the SMA enters into the IT-CMS all required data about the new or redeployed device. This information must be entered within ten working days of the input date of the requisition or the date of the redeployment decision.
 - If a change is required for an existing personal computer or network-connected computing device, the SMA enters into the IT-CMS all required data about that device. This information must be entered within ten working days of the date the SMA initiates the change.
- Reviews annually, at a minimum, information in the IT-CMS for each desktop for which he or she is responsible.
- Registers configuration parameters in the IT-CMS and updates them when they change. Those parameters are
 - IP name;
 - classification level of processed data;
 - ID of SMA and SO;
 - descriptive characteristics of device (e.g., manufacturer, model);
 - manufacturer of device;
 - type of device;
 - ID of device;
 - location of device, including site, building, and room; and
 - address of NIC.

Subject: Information Technology Configuration Management Instruction
--

2. PROGRAM STRATEGY AND IMPLEMENTATION (CONT.)

2.8 Personal Computing and Other Network-Connected Computing Devices, Associated Software, and Peripherals (cont.)

IST

- Designates an SMA for those devices with no assigned SMA. This may be accomplished by notifying the Directorate Computer Security Officer under whose jurisdiction the device resides and requesting an SMA assignment be made.
- Defines desktop business and technical requirements, including management requirements.
- Communicates annually with SMAs of record to require a review of the IT-CMS. The purpose of this review by the SMA is to verify the accuracy of the data for those desktop computing devices for which he or she is the designated SMA.
- Communicates changes in desktop computing business and technical requirements to all SMAs and SOs of record.

CTSO

- Reviews and approves or denies the ISSP for classified, UNSR, or other systems, as specifically designated by CTSO.
- Defines desktop computing security requirements. Security requirements are contained in Y19-401INS.

ISSO

- Prepares, reviews, and approves or denies the ISSP for classified, UNSR, or other systems, as specifically designated by CTSO.

ISSM

- Reviews and approves or denies the ISSP for classified and UNSR systems.

3. SOURCE DOCUMENTS

- *BWXT Y-12 Standards/Requirements Identification Document*
 - RUIDs 8105, 9663, 9752, 9754, 9757, and 9860
- DOE M 471.2-2, *Classified Information Systems Security Manual*
- DOE N 203.1, *Software Quality Assurance*
- DOE N 205.1, *Unclassified Cyber Security Program*
- Y15-004PD, *Configuration Management Program*
- Y19-401INS, *Automated Information System (AIS) Security Handbook*

Subject: Information Technology Configuration Management Instruction
--

4. RECORDS

The following records are generated and maintained according to established Y-12 records management practices and approved records inventory disposition schedules. See the Records Management and Document Control home page for more information.

- The SMA maintains UCN-20295.
- The SMA maintains a working copy of UCN-20297 for as long as necessary.
- IST maintains the record copy of UCN-20297.
- Records Management and Document Control maintains UCN-7721B.
- IOs, IMs, and SMAs maintain Web content as electronic records per Y-12 records management practices.
- The SO and SMA enter, maintain, and review data in the IT-CMS as described in this instruction. Some data may be obtained and maintained electronically via automated tools and is only reviewed.
- IST owns information contained in the IT-CMS and manages this information as electronic records per Y-12 records management practices.

Subject: Information Technology Configuration Management Instruction
--

APPENDIX A
Acronyms and Definitions
(Page 1 of 2)

ACRONYMS:

BWXT Y-12	BWXT Y-12, L.L.C.
C/TIO	Classification and Technical Information Office
CTSO	Computing and Telecommunications Security Organization
DOE	U.S. Department of Energy
ID	identification
IM	information maintainer
IO	information owner
IP	Internet Protocol
ISSM	Information System Security Site Manager
ISSO	information system security officer
ISSP	Information System Security Plan
IST	Information Systems and Technology
IT	information technology
IT-CMS	Information Technology Configuration Management System
NIC	Network Interface Card
NNSA	National Nuclear Security Administration
SMA	system manager/administrator
SO	system owner
UCNI	Unclassified Controlled Nuclear Information
UNSR	unclassified national security related
Y-12	Y-12 National Security Complex

DEFINITIONS:

Administrator—A person who is responsible for the custodianship and general management of a given information technology-related device.

Commercial-Off-The-Shelf—Software or hardware procured from a commercial third party (e.g., not created for custom use by Y-12 or Y-12 subcontractors) and generally used as-is after setup and configuration.

Desktop Computing Device—Any device that uses software to operate and is not dedicated to a specific function. For example, this typically is a personal computer used for business-support activities.

Information Maintainer—A person responsible for putting files on the Web server and for updating/removing files from the server as directed by the information owner.

Subject: Information Technology Configuration Management Instruction
--

APPENDIX A

(Page 2 of 2)

Information System Security Site Manager—An individual responsible for the establishment, documentation, implementation, and monitoring of the site classified information security program, including compliance with all U.S. Department of Energy/National Nuclear Security Administration requirements for information systems and technology. The ISSM functions as the site point of contact for all classified information security issues for information technology activities. The ISSM also reviews and approves Information System Security Plan (ISSP) documents and ensures the ISSP is implemented, including test results.

Networking Services Provider—A group of persons responsible for the maintenance and operations of a network under the guidance of the network manager. The provider's responsibilities include monitoring network activities, implementing network configuration changes, and designing and implementing additions or upgrades to the network.

Server—A computer or device on a network that manages network resources. A file server is dedicated to storing files. A Web server allows one to serve content over the Internet using hypertext markup language and other technologies. A print server manages one or more printers. A network server manages network traffic. A database server processes database queries. An application server serves applications to users and is used as a traffic cop in database-intensive situations. An e-mail server has a messaging system that allows users to exchange e-mail over local area networks and/or the Internet.

System Manager/Administrator—An individual responsible for maintaining a system in proper working order. For systems that serve multiple users (e.g., servers), this includes activities such as monitoring security configuration, managing allocation of user names and passwords, monitoring disk space and other resource use, performing backups, and setting up new hardware and software. For single-user systems (e.g., personal computer), this person typically is the primary user of the device.

System Owner—An individual responsible for providing business oversight to a designated system, such as a server, or the person who is the primary user of a system, such as a personal computer or other desktop device. For systems that serve multiple users (e.g., servers), this person frequently is a subject matter expert in the area in which the system resides (e.g., security, human resources). For single-user systems (e.g., personal computer), this person typically is both the owner of the device and the main user. This individual may authorize access by users of the system. This person also may provide requirements for the functionality of the system.