

No: Y15-405PD

Title: *Information Technology Configuration Management Program*

Rev: 04/04/02

This program description explains the Information Technology Configuration Management Program 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: Y15-405PD
Rev. Date: 04/04/02
Supersedes: New
Page: 1 of 15

BWXT Y-12
Management Control

Subject: Information Technology Configuration Management Program

Paul M. Parris /s/

Program description 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 Program

CONTENTS
(Page 1 of 1)

- 1. PURPOSE 4
- 2. SCOPE 4
- 3. STRATEGY 5
 - 3.1 Change Control..... 5
 - 3.2 Requirements Definition..... 6
 - 3.3 Document Control 6
 - 3.4 Assessments..... 7
 - 3.5 Organization and Administration 7
 - 3.6 Implementation 7
 - 3.6.1 Program Drivers 8
 - 3.6.2 Initial Implementation 8
 - 3.6.3 Level of Control..... 8
 - 3.6.4 Configuration Standards 8
 - 3.6.5 Life Cycle Strategy 9
- 4. REQUIREMENTS 9
- 5. ROLES AND RESPONSIBILITIES 10
 - 5.1 System Owner 10
 - 5.2 Information Owner 10
 - 5.3 System Manager/Administrator 10
 - 5.4 Information Maintainer 11
 - 5.5 Information Systems and Technology..... 11
 - 5.6 Computing and Telecommunications Security Organization..... 11
 - 5.7 Quality Assurance..... 11
 - 5.8 Maintenance Support..... 12
 - 5.9 Information System Security Officer..... 12
 - 5.10 Information System Security Site Manager 12
- 6. OTHER DOCUMENTS NEEDED 12
- 7. SOURCE DOCUMENTS 12
- 8. RECORDS 12
- APPENDIX A
Acronyms and Definitions..... 13

| |
|--|
| Subject: Information Technology Configuration Management Program |
|--|

REVISION LOG

(Page 1 of 1)

| Revision Date | Description of Change | Pages Affected |
|----------------------|---|-----------------------|
| 04/04/02 | This is a new document written to describe the Information Technology Configuration Management Program at the Y-12 National Security Complex in Oak Ridge, Tennessee. DM/R 02-15/405-001 has been completed to initiate this program description. | All |

| |
|--|
| Subject: Information Technology Configuration Management Program |
|--|

1. PURPOSE

The purpose of this program description is to provide information about the BWXT Y-12, L.L.C. Information Technology (IT) Configuration Management Program. This program governs the change process for computer hardware, software, and network items at the Y-12 National Security Complex (Y-12). The program

- provides requirements for identifying and documenting IT system components that are managed under the program;
- defines the process for controlling, adding, modifying, testing, and deleting IT components within the program throughout the component life cycle, including for both normal operational and emergency situations;
- establishes documentation, approvals, communication, reporting, and record retention requirements for IT components;
- defines configuration requirements for elements managed under the program;
- defines criteria for exceptions to standard configurations;
- defines a process for verifying the completeness and correctness of items managed under the program; and
- defines roles and responsibilities for the parties involved in the process.

Compliance with the IT Configuration Management Program ensures U.S. Department of Energy (DOE) and Y-12 configuration management requirements are met. New requirements will be incorporated into the program as necessary.

2. SCOPE

This program description 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 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; and
- personal computers and other network-connected computing devices, associated software, and peripherals.

This program description applies to components operating at any security classification level at Y-12, including unclassified, unclassified national security related, 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

| |
|--|
| Subject: Information Technology Configuration Management Program |
|--|

2. SCOPE (CONT.)

essential to the performance of various work activities at the site, 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 program description 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);
- 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.

3. STRATEGY

Within DOE, the following elements must comprise a configuration management program:

- change control,
- requirements definition,
- document control,
- assessments, and
- organization and administration.

These elements constitute a configuration management process and are, therefore, applied to the IT Configuration Management Program.

Specific requirements included in the IT Configuration Management Program will define a required level of control that addresses each of these elements. This may include control at the individual component level (e.g., server, network device, software program) or by component groupings using classes or other defined criteria. The use of the term “component” within this program description shall not be indicative of a required specific level of management granularity. The level of control, the criteria for components managed under the program, and requirements for implementation of the program are contained in Y15-406INS, *Information Technology Configuration Management Instruction*.

3.1 Change Control

Change control ensures changes are properly identified, reviewed, approved, implemented, tested, validated, and documented prior to use. Change control includes several critical elements.

- A change identification process is defined for identifying and approving, prior to implementation, changes to IT components and configurations covered by the program.

| |
|--|
| Subject: Information Technology Configuration Management Program |
|--|

3. STRATEGY (CONT.)

3.1 Change Control (cont.)

- A technical review and approval is required prior to implementation of designated changes to confirm the changes comply with requirements defined for each component.
- A management review is required prior to implementation of designated IT component changes.
- Changes to IT components and configurations are communicated to stakeholders prior to implementation. Changes are implemented via a defined process.
- Information regarding all changes is maintained for traceability of the change history over the life cycle of the component.
- Emergency changes are managed in compliance with the program.

3.2 Requirements Definition

Requirements define the physical, functional, operational, and performance capabilities of various components. This element interfaces with the change control component by providing a basis for determining the acceptability of changes. The requirements element also interfaces with the document control element of the program to ensure documentation on systems and changes is readily available. Requirements include several critical subelements.

- Design, installation, and operational requirements for components provide clear definition of the technical basis and implementation of the program. These requirements define the method for identifying components to be controlled within the program. Likewise, the design requirements define any standard configurations that must be in place for a component.
- All administrative requirements that apply to a component are clearly identified to support compliance by the component during its life cycle.
- Requirements are provided that define the integration of existing and legacy systems or components into the program.

3.3 Document Control

The document control element ensures documents—whether electronic or paper—used for decision making are kept current. The accuracy and availability of documents regarding a component are essential to successfully track change histories over an extended period. Document control includes the following critical steps:

- Identification—The documentation necessary to support configuration management of each component is identified. This may include paper, electronic, or other records (e.g., manufacturer's data). Documentation may be in any format as long as it remains accessible and retrievable for retention periods in accordance with Y15-101, *Records Management*, and the Comprehensive Records Schedule for Y-12.
- Control and Tracking—A methodology is defined for controlling and tracking changes to documentation related to components.

| |
|--|
| Subject: Information Technology Configuration Management Program |
|--|

3. STRATEGY (CONT.)

3.3 Document Control (cont.)

- Retrieval—Information related to items managed under the program is retrievable upon request by system owners (SOs), system managers/administrators (SMAs), or other parties who are responsible for the component under this program. Records for a component must have an identified repository and custodian so that information may be retrieved. This methodology should be consistent with Y15-102, *Document Control*. Y15-406INS defines specific repositories and custodians for records generated by this program.

3.4 Assessments

Independent and management assessments evaluate the existing configuration against the requirements and the relevant documents. Management assessments are performed by a manager or a manager's designee to determine the status of compliance with the identified function or operation of a component relative to requirements. At the request of a manager, independent assessments are performed by individuals not responsible for the function or operation of the component being addressed for requirements compliance. Examples of assessments include Physical Configuration and Periodic Equipment Monitoring.

In a Physical Configuration Assessment, a process is defined for assessing compliance with the existing records and mandated configurations for each component. This process may include physical walkdowns, electronic monitoring, targeted audits, and other methods. This ensures the program is being followed by assessing the status of components at a point in time against the records regarding that component.

A Periodic Equipment Monitoring Assessment involves defining a process for ensuring each component meets current technical and administrative requirements. This verifies components actually are performing as required by the program.

3.5 Organization and Administration

The organization and administration element manages the overall IT Configuration Management Program and supports the program's implementation in a cost-effective and consistent manner.

3.6 Implementation

The IT Configuration Management Program will be implemented via Y15-406INS, which describes requirements and processes for each area covered within the scope of this program description. Specific implementation guidance or additional management requirements also will be provided for components requiring standard configurations. This information can be found on the Information Systems and Technology (IST) organization home page on the internal Web server.

| |
|--|
| Subject: Information Technology Configuration Management Program |
|--|

3. STRATEGY (CONT.)

3.6 Implementation (cont.)

3.6.1 Program Drivers

Configuration management as a requirement of the Y-12 Quality Program is a key driver for the IT Configuration Management Program. IT hardware and software components are enabling tools that assist in performing work at Y-12. These components not only support work at Y-12 but also serve as part of the actual implementation of overall information and computer security requirements at the site. A failure in configuration management for IT components can result in an unacceptable breakdown in quality and/or security for Y-12. Therefore, these components must be managed in a fashion that complies with overall Y-12 Quality Program and security requirements so that employees at Y-12 can perform their work safely and securely.

3.6.2 Initial Implementation

As of the implementation date of this program, certain IT components may not be covered by an existing Y-12 configuration management program or may be covered by other local programs. For those components, which are covered by the scope of this new program, an implementation plan is provided to support “grandfathering” of these items. This plan can be found on the internal Web server at the IST organization’s home page. For all other new components covered by this program, coverage begins immediately upon introduction of the component into the Y-12 environment.

3.6.3 Level of Control

The IT Configuration Management Program is controlled in a tiered manner. IST manages the overall program. The Computing and Telecommunications Security Organization (CTSO) and the Quality Assurance organization are responsible for integrating Y-12 computer security and quality requirements into the program in an ongoing manner. Individual IT areas (e.g., computing desktops, servers, Web pages) have identified owners for each component that is under configuration management. These owners are responsible for ensuring the component is managed in compliance with the program. In most cases, the component owner who is responsible for compliance is the person at Y-12 with day-to-day oversight of that component. As an example, the owner of a desktop personal computer typically is the user. Similarly, for a server, the owner typically is the individual with daily responsibility for the services provided by the system (e.g., security, engineering design support).

3.6.4 Configuration Standards

Certain components managed under this program have mandatory configuration standards. These standards are defined within information provided on the internal Web server at the IST organization’s home page or in Y15-406INS. Configuration standards assist with maintaining consistency across Y-12 for these components. This further aids in auditing, record-keeping, implementation, and other activities. Configuration standards do not apply to all IT components, due to the dynamic and varied nature of some items.

| |
|--|
| Subject: Information Technology Configuration Management Program |
|--|

3. STRATEGY (CONT.)

3.6 Implementation (cont.)

3.6.5 Life Cycle Strategy

As with other systems, successful configuration management of IT components falls into two key areas—the initial process of developing or procuring and installing a component to meet configuration management guidance and the ongoing configuration change process over the component's lifetime. The latter requires that the proper configuration profile be maintained during that period. For successful management, cradle-to-grave oversight is performed. The IT Configuration Management Program addresses all of these areas.

3.6.5.1 Information Technology Configuration Management System (IT-CMS)

Support systems and tools will be defined and implemented to augment the configuration management process at Y-12. These systems and tools may be a combination of existing systems and those developed as part of establishing the program at the site. Together, these systems and tools will constitute the IT-CMS. The roles and responsibilities within the IT-CMS will be consistent with those described in Section 5 of this document.

3.6.5.2 Standard Workflow

The IT Configuration Management Program will implement a standard, basic approach to oversee items covered by the program at Y-12. Typically, the process involves four steps, which are defined in this section. These steps are intended as paradigms, and specific requirements will be defined in Y15-406INS.

- 1) Change proposal—A change to the existing baseline is proposed. This may include modifications to an existing item, the addition of a new item, or a deletion. The proposed change is entered into the IT-CMS for review.
- 2) Change review—Responsible parties [e.g., information maintainer (IM), information owner (IO), CTSO] perform a review within the IT-CMS. All changes requiring approvals typically follow a predefined workflow based on the owner designated for the item within the IT-CMS.
- 3) Change approval/denial—For those changes that have a review, the reviewing parties either approve or deny the proposed change within the IT-CMS.
- 4) Change implementation/testing—For approved changes, a system manager/administrator (SMA), IM, Maintenance staff member, or other qualified party performs a technical implementation.

4. REQUIREMENTS

This document establishes tasks to be performed when implementing configuration management requirements derived from several sources. Software-related requirements are detailed in accordance with Y80-101PD, *Software Management Program Description*, and DOE N 203.1, *Software Quality Assurance*. Security requirements are based on

| |
|--|
| Subject: Information Technology Configuration Management Program |
|--|

4. REQUIREMENTS (CONT.)

DOE M 471.2-2, *Classified Information Systems Security Manual*, DOE N 205.1, *Unclassified Cyber Security Program*, and Y19-401INS, *Automated Information System (AIS) Security Handbook*. The general approach to configuration management is derived from Y15-004PD, *Configuration Management Program*. Several *BWXT Y-12 Standards/Requirements Identification Document* entries also apply and are listed in Section 7.0.

5. ROLES AND RESPONSIBILITIES

The following sections describe the roles of individuals or organizations in implementing the Y-12 IT Configuration Management Program. The duties listed are not all-inclusive, and more detail may be provided in the management requirement (i.e., Y15-406INS) that implements the program. Other roles may be identified within the guidance provided on the internal Web server at the IST organization's home page. In the event guidance provided on the Web and in Y15-406INS contradict, Y15-406INS shall prevail. See Appendix A for definitions of the roles described in the following sections.

5.1 System Owner (SO)

The SO primarily is responsible for overall compliance with the IT Configuration Management Program. The SO's responsibilities include

- identifying new and existing IT components within the program and updating information as changes occur,
- inputting component changes not maintained via automated tools into the systems that implement the program, and
- following configuration standards or design requirements defined within the program.

5.2 Information Owner (IO)

The IO is responsible for compliance with the IT Configuration Management Program for information collections, specifically those hosted on Web servers. The IO's responsibilities include obtaining approval of all site content via the required approval process and defining, reviewing, and registering all information areas with IST.

5.3 System Manager/Administrator (SMA)

The SMA is responsible for carrying out program guidance in daily operational management of components covered by the program. Responsibilities of the SMA include

- installing, configuring, testing, implementing, and maintaining components in accordance with the program;
- implementing only approved component changes;
- updating or maintaining selected information regarding component changes or configuration; and
- following configuration standards or design requirements defined within the program.

| |
|--|
| Subject: Information Technology Configuration Management Program |
|--|

5. ROLES AND RESPONSIBILITIES (CONT.)

5.4 Information Maintainer (IM)

The IM primarily is responsible for maintaining Web files on a Web server.

5.5 Information Systems and Technology (IST)

IST has overall ownership of the Y-12 IT Configuration Management Program and is responsible for its administration. IST's responsibilities include

- maintaining the program in accordance with Y-12 and DOE/National Nuclear Security Administration (NNSA) standards, including defining requirements;
- performing periodic assessments to confirm proper program implementation;
- providing support systems, as necessary, to implement the program;
- publicizing the program to IT stakeholders;
- providing standard configurations for selected technology components covered by the program;
- maintaining documentation related to the program; and
- providing technical solutions (e.g., tracking changes or documents) to implement the program.

5.6 Computing and Telecommunications Security Organization (CTSO)

CTSO is responsible for ensuring computer security requirements are incorporated into the program and security audits are performed on selected components. The responsibilities of CTSO include

- incorporating DOE/NNSA security requirements into the implementation of the program and its base requirements,
- performing security assessments for proper implementation of program security guidance,
- verifying standard configurations for technical components covered by the program are in accordance with security requirements,
- providing and approving guidance on the implementation of security changes for components covered by the program, and
- reviewing and approving selected changes to components covered by the program prior to implementation.

5.7 Quality Assurance

The Quality Assurance organization is responsible for ensuring Y-12 Quality Program requirements contained in Y60-101PD, *Quality Program Description*, are incorporated into this configuration management program and for providing oversight of the quality assurance requirements incorporated into this program.

| |
|--|
| Subject: Information Technology Configuration Management Program |
|--|

5. ROLES AND RESPONSIBILITIES (CONT.)

5.8 Maintenance Support

Maintenance Support staff are responsible for ensuring defined modifications to components managed within the program, including those made during installation and configuration, are made in compliance only with proper approvals and within program guidance.

5.9 Information System Security Officer (ISSO)

The ISSO is responsible for participating in the computer security process in conjunction with CTSO. The ISSO's responsibilities include working in conjunction with the SMA and SO to define secure system configurations and preparing, reviewing, and maintaining Information System Security Plans.

5.10 Information System Security Site Manager (ISSM)

The ISSM is responsible for implementing Y-12's classified information security program and ensuring appropriate elements of that program are incorporated into the IT Configuration Management Program. The ISSM also is responsible for approving changes to classified systems.

6. OTHER DOCUMENTS NEEDED

- Y15-101, *Records Management*
- Y15-102, *Document Control*
- Y15-406INS, *Information Technology Configuration Management Instruction*
- Y80-101PD, *Software Management Program Description*

7. 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*

8. RECORDS

No records are generated as a result of following this program description.

| |
|--|
| Subject: Information Technology Configuration Management Program |
|--|

APPENDIX A
Acronyms and Definitions
(Page 1 of 3)

ACRONYMS:

| | |
|--------|--|
| CTSO | Computing and Telecommunications Security Organization |
| DOE | U.S. Department of Energy |
| IM | information maintainer |
| IO | information owner |
| ISSM | Information System Security Site Manager |
| ISSO | Information System Security Officer |
| IST | Information Systems and Technology |
| IT | information technology |
| IT-CMS | Information Technology Configuration Management System |
| NNSA | National Nuclear Security Administration |
| SMA | system manager/administrator |
| SO | system owner |
| Y-12 | Y-12 National Security Complex |

DEFINITIONS:

Change Control—The tracking and management of changes made to specified components of a system. See “Configuration Management.”

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.

Configuration Management—The process of applying technical and administrative controls to (a) identification and documentation of physical and functional characteristics of configuration items, (b) any changes to characteristics of those configuration items, and (c) recording and reporting of change processing and implementation of modifications to systems that contain these configuration items.

Document Control—Administrative controls for the generation, revision, release, receipt, distribution, disposition, and file maintenance of documents, regardless of media used. These controls ensure documents selected for control are reviewed for adequacy, approved for release by authorized personnel, and distributed to identified controlled document holders for use.

Firmware—Software stored in read-only memory or programmable read-only memory. Firmware often is responsible for the behavior of a system when it first is switched on.

Subject: Information Technology Configuration Management Program

APPENDIX A

(Page 2 of 3)

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.

Information Owner—An individual responsible for providing business oversight to a designated collection of Web-based information content. Frequently this person is subject matter expert in the area in which the information resides (e.g., security, human resources). Typically this individual may authorize access by system users to the information.

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.

Information Technology—Applied computer systems (both hardware and software and including networking and telecommunications) in the context of a business or other enterprise.

Server—A computer that provides some service for other computers connected to it via a network. The most common example is a file server that has a local disk and services requests from remote clients to read and write files on that disk.

Software—Computer programs, procedures, and associated documentation and data pertaining to the operation of a software product or system. Software includes applications, operating systems, software routines and macros, firmware, programmable logic controller ladder diagrams, measuring and test equipment-associated software, and exploratory projects.

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.

Subject: Information Technology Configuration Management Program

APPENDIX A

(Page 3 of 3)

Walkdown—A physical review and inspection of a system or selected system components, intended to identify problems or concerns or assess compliance with standards.