NATIONAL WEATHER SERVICE INSTRUCTION 30-1203
JANUARY 23, 2012

Maintenance, Logistics, and Facilities

Configuration and Data Management, NWSPD 30-12

CONFIGURATION MANAGEMENT FOR OPERATIONAL SYSTEMS

NOTICE: This publication is available at: http://www.nws.noaa.gov/directives/.

OPR: W/OPS13 (M. DeTommaso) **Certified by:** W/OPS (M. Paese)
Type of Issuance: Routine.

SUMMARY OF REVISIONS: This Procedural Directive supersedes National Weather Service (NWS) Procedure Directive 30-1203, dated September 30, 2003, and includes NIST 800-53 Configuration Management requirements.

Signed January 9, 2012
Mark Paese Date
Director, Office of Operational Systems

NWS Directives System - Configuration Management for Operational Systems

Table of Contents:

1 Purpose. The Federal Information Security Management Act (FISMA) requires agencies to establish "minimally acceptable configuration requirements." NWS policy 30-12 establishes Configuration Management (CM) policy for NWS systems. CM is comprised of a collection of activities focused on establishing and maintaining the integrity of products and systems through the control of the processes for initializing, changing, and monitoring the configuration of those products and systems.[1] The practice of CM is comprised of the following elements:

a) Configuration Item Identification - the methodology for selection and naming identifiable items that need to be placed under CM. CIs are the discrete target of configuration control processes.

b) Baseline Configuration Management – process for establishment and management of the baseline configuration for the identified CIs.

c) Configuration Change Control - the processes for managing updates to the baselines for CIs.

[1] From NIST 800-128 (DRAFT), Guide for Security Configuration Management of Information Systems, March 2010, page 6.

d) Configuration Monitoring – a process for assessing or testing the level of compliance with the established configuration baseline and mechanisms for reporting on the configuration status of items placed under CM.

CM disciplines allow you to revise system capabilities, improve system performance, extend system life, reduce system costs, minimize risk or liability, and correct system defects. Not placing a system under CM control, or lack of adherence to established CM procedures, can result in:

(1) Excessive costs due to extensive engineering design changes;
(2) Unwarranted hardware and software repairs;
(3) Catastrophic hardware or software system failures, impacting the NWS' ability to perform its primary mission of protecting life and property, and/or
(4) FISMA violations.

2 Scope of Configuration Management. The Director of the Office of Operational Systems (OPS) is responsible for designating operational systems under CM control. For these systems, the CM discipline will follow NIST 800-53 and encompass the following controls[2]:

- CM-1 Configuration Management Policy and Procedures – establishes a formal documented configuration management policy that addresses purpose, scope, roles, and responsibilities.
- CM-2 Baseline Configuration - requires development, documentation, and maintenance of a baseline under configuration control.
- CM-3 Configuration Change Control –determines the type of changes that are configuration controlled, as well as establishes processes for the documentation, retention, coordination, approval, and audit of these changes.
- CM-4 Security Impact Analysis – requires changes to be analyzed to determine potential security impacts prior to implementation.
- CM-5 Access Restrictions for Change – requires definition, documentation, approval and enforcement of physical and logical access restrictions associated with system changes.
- CM-6 Configuration Settings – requires the establishment of mandatory configuration settings, as well as exceptions from these settings, and the documentation, implementation, monitoring, and control of changes to these settings.
- CM-7 Least Functionality – requires configuration of only essential capabilities for the system.

[2] NIST 800-53 Recommended Security Controls for Federal Information Systems and Organizations, Revision 3, August 2009.

- CM-8 Information System Component Inventory – requires the documentation and maintenance of an inventory of system components that accurately reflects the current system, and is at a level of necessary granularity consistent with the system authorization boundary.
- CM-9 Configuration Management Plan – requires documentation and implementation of a configuration management plan that defines configuration items, system specific CM processes and procedures, and processes for managing the baseline.

3 Process to Establish CM Control. OPS CM organizations work with System Owners to implement CM controls. A CM baseline is established in conjunction with the OPS Director/Authorization Official issuance of an Authority to Operate decision. The CM controls required are based on the system's Federal Information Processing Standard (FIPS) 200 security classification (low, moderate, or high). CM organizations for OPS systems are provided in Section 4.

4 Systems under Configuration Management. The OPS Director has designated CM control for the following operational systems:

Table 4-1 OPS Designated System under CM Control

System Name	**CM Responsible Organization**	**System Owner**
Automated Surface Observing System (ASOS)	OPS13	OPS22
NWS Internet Dissemination System (NIDS)	OPS13	OPS13
NEXRAD (WSR88D)	OPS42	OPS4
NOAA Weather Radio	OPS13	OPS17
OPSnet	OPS13	OPS34
Upper Air	OPS13	OPS22
Telecommunication Gateway	OPS13	OPS3

Any systems transferring to OPS will follow this standard.

5 National CM Processes. CM is handled across multiple organizations within OPS. The Configuration Branch, (W/OPS13) is responsible for all CM controls for systems managed at OPS Headquarters in Silver Spring, MD. Appendix A describes the responsibilities of the Configuration Branch.

The Program Branch, (W/OPS42) in the OPS Radar Operations Center, is responsible for all CM controls for the NEXRAD. Appendix B describes the responsibilities of the Program Branch.

5.1 Change Control Process. For systems under OPS Configuration Management control, a change request is approved before any change can be made. However, Electronic Systems Analysts (ESAs) and Regional Headquarters Meteorologists In Charge (MIC) may authorize temporary modifications to restore critical system(s) operation in an emergency. After the emergency, a change request is initiated or the system is restored to its original configuration. Each ESA will ensure all systems remain standardized under NWS CM policy and prescribed configuration.

Full re-certification and accreditation, including issuing a new Authority to Operate decision, occurs whenever there is a significant system change and is as described in the system Configuration Management Plan document for Moderate and High systems or within the System Security Plan (SSP) in the Configuration Management (CM) family of controls for a Low system. The definition of "significant change" is relative to the business case outlined in the business impact analysis of the particular system in question. A significant change includes, but is not limited to:

- Changing to a new system architecture or system environment affecting the entire system or a significant portion of the system whereupon said change impacts the day-to-day operation of the system;
- Installation of a new operating system, middleware component, or major application that affects the entire system or a significant portion of the system whereupon said change impacts the day-to-day operation of the system;
- Installation of a new hardware platform; and / or
- Changes in the system FIPS-199 classification or within the authorization boundary of the information system.

The significant change is applied to the individual system, is defined by the System Owner, and is captured in the Configuration Management Plan established for the system. Please note that the definition of a "significant change" varies from system to system unless two systems outline the identical business case and operating environment. For the most part, a significant change can be looked upon as a change that negatively impacts the FIPS 199 rating of Confidentiality, Integrity, and/or Availability for that particular system. Please see the definition of significant change as outlined in the system Configuration Management Plan and/or as defined in the CM control family in the SSP.

5.2 Engineering Management Reporting System. The Engineering Management Reporting System (EMRS) is used to obtain completed configuration change information for field maintained systems under CM control. Please refer to NWS Instruction 30-2104, Maintenance Data Documentation for instructions on using EMRS. The ESA is responsible for coordinating, managing, validating, and recording all configuration changes (e.g., modifications, requests for

change, maintenance notes) to assigned systems performed by Government and/or contractor personnel. The ESA is also responsible for ensuring accountability for the coordination, management, validation, completion, and EMRS submission of each configuration change.

5.3 Contract Administration for Equipment under CM Control. The Program Manager for the equipment contract is responsible for coordinating CM sections of the contract Statement of Work (SOW), with OPS CM whenever a new SOW is being created for equipment under configuration control or whenever a SOW for equipment under configuration control has been modified. OPS CM will review and provide comment on the CM sections of the SOW, including contract deliverables.

6 Locally Administered CM Procedures. If a NWS Headquarters Office Director, Region Director, or the Director for National Centers for Environmental Prediction chooses to administer their own CM procedures for a system, or any part thereof, they provide a mechanism to document the NIST 800-53 CM controls. Locally administered CM procedures are documented in supplemental procedural directives to this national directive. OPS reviews proposed supplemental CM procedural directives to ensure they comply with national CM requirements and avoid unnecessary duplication of efforts.

7 References. The following references also contain greater detail.

NWSI 10-101, Change Management Process.

APPENDIX A. – Configuration Branch Responsibilities

Table of Contents: Page

1 Configuration Branch (OPS13). The Configuration Branch Chief is responsible for implementation of all CM controls for operational systems listed in Section 4 under its CM control. The Configuration Branch Chief is responsible for the following CM controls:

a) Developing and documenting policies stating CM purpose, scope, roles, responsibilities, and procedures to facilitate the implementation of NWS CM policy.

b) Documenting the System Production Baseline consisting of all constituent components, and ensure the baseline documentation is updated annually, or when updates occur.

c) Documenting the types of changes that are configuration controlled, i.e., "significant changes" via NWS Terms of Reference documentation and the particular system documentation as outlined in Section 5.1.

d) Documenting the System ISSO has reviewed risk impacts for all changes.

e) Documenting the physical and logical access restrictions for the system.

f) Documenting the mandatory and restrictive settings for the system, and any exceptions to these settings.

g) Documenting that the information system has been configured to provide only essential capabilities (specifically prohibiting functions, ports, protocols and services).

h) Documenting the component level inventory within the accreditation boundary

i) Documenting Configuration Items, CM roles, responsibilities and procedures using the NOAA CM Plan Templates.

j) Developing automated CM programs on the Configuration Branch Information Technology System, as needed.

OPS13 will work with System Owners to establish a CM checklist covering the necessary NIST 800-53 CM controls, depending on the System Security classification.

APPENDIX B. – Radar Operations Center Program Branch Responsibilities

Table of Contents: Page

1 Radar Operations Center Program Branch (OPS42). The Radar Operations Center (ROC) Program Branch, CM Team, develops and maintains effective and efficient CM processes and is responsible for Configuration Identification, Configuration Control, Configuration Status Accounting, and Configuration Audits of the NEXRAD Generation Radar System (WSR-88D). The ROC Program Branch, CM Team, manages the WSR-88D tri-agency change process and provides the administrative and technical structure in support of the tri-agency Configuration Control Board.

The Configuration Management Team will:

a) Ensure the life-cycle management of WSR-88D System Configuration and its associated technical data package.

b) Ensure the accuracy of the WSR-88D engineering drawings, associated lists, and baseline specifications.

c) Establish and maintain the NEXRAD Technical Data Repository to include the Agile Configuration Status Accounting System, Razor Software Configuration Management System, and the Dynamic Object-Oriented Requirements System (DOORS). Agile is used for hardware Configuration Control and Configuration Status Accounting. Razor is used for Software Configuration Control, Configuration Status Accounting, and Build Management. DOORS manages system, functional, performance, design, and test requirements at all levels.

d) Incorporate changes, generated by approved Engineering Change Proposals (ECPs), Engineering Change Orders (ECOs), and Specification Change Notices (SCNs), into the WSR-88D Technical Data Package.

e) Track and facilitate configuration changes through the review cycle.

f) Control the hardware and software product baselines for the system and network.

g) Conduct Configuration Audits to ensure the integrity of the WSR-88D System Baselines.

h) Establish a cost-effective and efficient closed-loop Software Build, Release, and Distribution System for WSR-88D System Software.

The ROC Program Branch Chief will act as the final releasing authority for the baseline technical documentation.