NATIONAL WEATHER SERVICE INSTRUCTION 30-1203
October 2, 2018

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/OBS32 (T. Day) **Certified by:** W/OBS3 (M. Miller)

Type of Issuance: Routine

SUMMARY OF REVISIONS: This instruction supersedes National Weather Service (NWS) Instruction 30-1203, *Configuration Management for Operational Systems*, dated January 23, 2012. Changes were made to reflect the NWS Headquarters reorganization, effective April 1, 2015. Other revisions included:

1. Inclusion of an Introduction Section (page 2)
2. Updated Configuration Management (CM) process (Section 4, page 5) including the following:
    1) Identified the CM Baseline process (Section 4.1, page 5)
    2) Provided information on Configuration Status Accounting Section 4.2, page 5 including Configuration Management Information System (CMIS) (Section 4.2.1, page 6) and the Document Management System (DMS) (Section 4.2.2, page 6)
    3) Provided information on CM Change Control (Section 4.3, page 6)
    4) Updated the Configuration Validation and Audit review process (Section 4.4, page 6)

//Signed// 9/18/18

Joseph A. Pica Date

Director, Office of Observations

Table of Contents

1. Introduction

National Weather Service Instruction (NWSI) 30-1203 establishes Configuration Management (CM) guidance for Operational Systems and NWS-owned facilities. NWS 30-1203 directs the processes required to implement CM disciplines in accordance with EIA 649B and NIST 800-53 Rev4. CM Controls.

2. Purpose

This instruction adheres to the Federal Information Security Management Act (FISMA) that requires agencies to establish "minimally acceptable configuration requirements." NWS policy 30-12, *Configuration and Data Management"* that 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 by controlling the processes for initializing, changing, and monitoring the configuration of those products and systems. The following elements are included in the CM process:

1. Configuration Item Identification (CI) - the methodology for selecting and naming identifiable items that need to be placed under CM. CIs are the discrete target of configuration control processes.
2. Baseline Configuration Management – process for establishing and managing the baseline configuration for the identified CIs.
3. Configuration Change Control - the processes for managing updates to the baselines for CIs.
4. 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.
5. Security Focused Configuration Management (SecCM) – the management and control of configurations for information systems in order to enable security, and to facilitate the management of information security risk. Security-focused configuration management is used to emphasize the concentration on information security.
6. Audit and Review- the process of auditing and reviewing program system configuration items relative to the approved configurations throughout the program life cycle to ensure baseline integrity and compliance.

The CM process allows revisions to system capabilities, improvements in system performance, extension in system life, reduction in system costs, minimization of risk or liability, and correction of system defects. If a system is not placed under CM control, or if established CM

procedures are not followed, then this 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.

(4) Unreported or managed system weakness and flaws leading to security breaches, unauthorized disclosure or disruption of service.

(5) Regulatory and/or policy violations (FISMA, OMB, DOC, NWS, and others).

3. Scope of Configuration Management

The Director of the Office of Observations (OBS) in coordination with the Office of Dissemination, is responsible for designating operational systems under CM control. For these systems, the OBS32 Services Branch CM will follow Industry Standard EIA 649, *National Consensus Standard for Configuration* Management, and NIST 800-53, *Assessing Security and Privacy Controls In Federal Information Systems and Organizations*.

EIA Standard 649 defines a balanced and continuous application of CM functions and their underlying principles throughout the product lifecycle. It identifies the following CM principles for a product:

1. Configuration Management Planning- Delineates the specific CM application methods and their levels of emphasis, providing an understanding of the context and the environment of the product/system to which the CM process(es) is applied.

2. Configuration Identification- Provides the basis from which the configurations of products are defined, labeled and documented. Product configuration information serves as the baseline foundation for development, production, operation, and maintenance/support of the product/system, and various lifecycles that the CI process is utilized in.

3. Configuration Change Management- Provides systematic and measurable change process to manage both changes and variances from the approved product or system configuration information.

4. Configuration Status Accounting- Provides an accurate baseline of the product/system as it evolves and is maintained throughout the lifecycle.

5. Configuration Verification and Audit- Verifies a product or system's compliance with the physical, functional, and interface requirements in the approved

product/system definition confirming the applicable baseline.

NIST 800-53 defines CM security controls to be applied to all operational Information Technology Systems and identifies and encompasses the following controls for compliance to Office of Management and Budget (OMB) security requirements:

1. CM-1 Configuration Management Policy and Procedures – Establishes a formal documented configuration management policy that addresses purpose, scope, roles, and responsibilities.
2. CM-2 Baseline Configuration - Requires development, documentation, and maintenance of a baseline under configuration control.
3. 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.
4. CM-4 Security Impact Analysis – Requires changes to be analyzed to determine potential security impacts prior to implementation.
5. CM-5 Access Restrictions for Change – Requires definition, documentation, approval, and enforcement of physical and logical access restrictions associated with system changes.
6. 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.
7. CM-7 Least Functionality – Requires configuration of only essential capabilities for the system,
8. 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.
9. 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.

4. Establishing CM for System Lifecycle Management

Configuration Management is employed at the beginning of the program's system lifecycle. It is an ongoing lifecycle process sustained through the evolution of baseline development and change

control.

4.1 Configuration Baseline

The Configuration Baseline process is an evolutionary process with the established functional and allocated baseline of Systems Requirements, Critical Design documentation, and final design validation of Product Identification Documentation. Baseline milestones are critical to successful execution and product development. Short cutting these steps is detrimental to the production and ongoing support of products and equipment through production and operational lifecycles. Execution of baseline milestones is critical to an orderly evolution and support of product upgrades, design changes, logistics, and maintenance support during the product's lifecycle. NWS OBS 32 Services CM will accommodate all levels of baselining and will provide the Technical Reference Library (TRL) Document Management System (DMS). A product baseline is formalized and formal Change Control is mandatory upon the completion and approval of the Functional Configuration Audit (FCA) and Physical Configuration Audit (PCA). The formal product baseline should coincide and be approved in conjunction with the Director/Authorization Official's issuance of an Authority to Operate (ATO) decision. The required CM controls are based on the system's Federal Information Processing Standard (FIPS) 200 security classification (low, moderate, or high).

For systems under CM control, Configuration Management Plans are required to satisfy NIST 800-53 CM-1 and CM-9 controls.

4.2 Configuration Status Accounting

Critical to CM baselining is the establishment of Configuration Status Accounting (CSA). CSA is established to record baselined configuration data and associated lists (e.e. part lists, bills of materials and engineering drawing attribute data). All baseline documentation and status is released to the OBS32 Services CM Document Management System (DMS). Engineering Design Drafting tools are also integrated into CMIS to allow integrated drawing release engineering change and change Associate Lists are generated via the Configuration Branch Information System (CMIS). CMIS is the primary SCA application hosting all primary Configuration Status Accounting data for system component and piece part lifecycle evaluation and identification of system configuration, parts, and associated locations.

4.2.1 Configuration Management Information System (CMIS)

The Configuration Management Information System (CMIS) allows portal access to NOAA project members, Engineering, Maintenance, and Logistics to include field support personnel. CMIS provides CSA database maintenance applications and provides project specific baselined

Engineering Drawing and Associated List access exported directly from the Document Management System (DMS). CMIS produces Part List in accordance with Industry Standard ASME Y14.34M Associated Lists.

4.2.2 Document Management System (DMS)

The Document Management System (DMS) provides formal orderly release of engineering documentation baselines and in-process drawing and data. DMS is integral to the engineering design and document release process. DMS provides Associated List IAW Industry Standard ASME Y14.34M Associated Lists.

4.3 Change Control

Change Control is implemented on NWS systems through the Request for Change (RC) system. The Request for Change system is defined in NWS Instruction 30-1205 *Change Management*.

4.4 Configuration Validation and Audit

OBS32 CM shall organize and lead the CM audit and review process that includes establishing the entry and exit criteria and executing procedural steps.

OBS32 CM will initiate formal and ad-hoc configuration audits as necessary to assure the integrity of the system baseline documentation and physical system configuration.

4.4.1 Entry Criteria for the Functional Configuration Audit or Physical Configuration Audit

The following list identifies the entry criteria for a Functional or Physical Configuration Audit:

1. Create audit documentation that consists of the following:
    1) Action Items
    2) List of responses and resolutions to action items
    3) Audit Report and minutes
2. Execute Audit Plan of action that includes the following:
    1) Create summary of the Functional Configuration Audit
    2) Document test procedure and results
    3) Review deviations an waivers

4) Create summary of the Physical Configuration Audit

5) Develop product baseline, if required

6) Review and validate specifications

7) Review drawing

8) Conduct review of shortages and unincorporated design changes

9) Create proposed system acceptance documentation

10) Review contractor's Engineering Release and Change Control System

11) Review As-built List (drawings or configuration list)

12) Review logistics support plan for pre-operational support

13) Review long lead time and provisioned items

3. Create the audit closure documentation that consists of the following:

1) Documents that were not available at time of system acceptance

2) Audit minutes/reports

4.4.2 Exit Criteria for the Functional Configuration Audit or Physical Configuration Audit

The following list identifies the exit criteria for a Functional or Physical Configuration Audit.

1. Sign-off of all audit action items and documentation deliverables.
2. Resolution of audit discrepancies that were documented through an action item.
3. Review and sign-off of audit closure documentation sheets by the CM and technical representative.
4. Provision of audit minutes and/or report to the Project Manager.

5. Systems under Configuration Management

The OBS32 Services Branch CM organization works with Program Managers and System Owners to implement CM controls. The OBS Director has designated CM control for the following operational systems:

Table 1 OBS Designated System under CM Control

System Name	CM Responsible Organization

Automated Surface Observing System (ASOS)	OBS32-3
NEXRAD (WSR88D)	OBS
NOAA Weather Radio	OBS32-3
Upper Air	OBS32-3

6. National CM Processes

CM is handled across multiple organizations within OBS, the Configuration Branch (OBS32), and the Program Branch in the OBS Radar Operations Center (ROC). OBS32 is responsible for all CM controls for systems managed at NWS Headquarters in Silver Spring, MD. The Program Branch in the OBS Radar Operations Center is responsible for all CM controls for the NEXRAD. Refer to Appendix A for the responsibilities of the Configuration and to Appendix B for the responsibilities of the Program Branch.

6.1 Change Control Process

For systems under OBS Configuration Management control, a change request is approved before any change can be made. Please refer to NWS Instruction 10-103, *Operations and Services Improvement Process Implementation*, for information pertaining to the NWS Change Management process. 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, either 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 policyand prescribed configuration.

NIST 800-53 requires full re-authorization, including issuing a new Authority to Operate decision, and this, 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 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:

1. 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.
2. 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.

3. Installation of new hardware platform.

4. 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.

6.2 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.

6.3 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 OBS32 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. OBS32 CM will review and provide comment on the CM sections of the SOW, including contract deliverables.

7. 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, NWSPD 30-12, *Configuration and Data Management*. OBS Services Branch CM reviews proposed supplemental CM procedural directives to ensure they comply with national CM requirements and avoid unnecessary duplication of efforts.

8. References

The following documents can be referred to for more information:

NWS Policy Directive 30-12, *Configuration and Data Management*

NWS Instruction 30-1205, *Change Management Process*

APPENDIX A. – Configuration Team Responsibilities

The OBS32 Services Branch CM is responsible for the operational systems listed in Table 1, *OBS Designated Systems Under CM Control*. This includes the following controls:

1. Develop and document policies stating CM purpose, scope, roles, responsibilities, and procedures to facilitate the implementation of NWS CM policy.
2. Provide CM guidance during the NWS acquisition process to ensure adequate CM practices and data requirements are employed. Document the system baselines consisting of all constituent components, and ensure the baseline documentation is maintained over the lifecycle of the product or system.
3. Design and maintain the Configuration Management Information System (CMIS) containing configuration identification, baseline documentation, site configuration, and authorizing change document information. Compile Master Program Bills of Materials for Full Lifecycle Support.
4. Document 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 6.1.
5. Document the System ISSO has reviewed risk impacts for all changes.
6. Document the physical and logical access restrictions for the system.
7. Document the mandatory and restrictive settings for the system, and any exceptions to these settings.
8. Document that the information system has been configured to provide essential capabilities (specifically prohibiting functions, ports, protocols and services).
9. Ensure close-loop implementation of configuration of changes affecting baseline equipment and documentation.
10. Document the component level inventory within the accreditation boundary in concert with Configuration Status Accounting for the product/system.
11. Document Configuration Items, CM roles, responsibilities and procedures using the NOAA CM Plan Templates.
12. Develop automated CM programs on the Configuration Branch Information Technology System, as needed.
13. Conduct Functional and Physical Configuration Verification and Audits as required by system lifecycle phases, project schedule, and configuration change.
14. Maintain the software CM repository of production software using a 3rd party

software development model. To perform this responsibility, OBS 32 Services Branch CM needs to validate a software Listing package for each new software release for systems under CM control. The Software Listing package will include a DAT tap/CD of all source code, compilation tools, scripts, and any other software that makes up the complete software load. In addition, the Software Listing package will include the Version Description Document, all new requirements, and any discrepancy documentation/trouble reports to provide a complete validation review and accountability package for the new version of software. The responsible software development organization is responsible for delivering the Software Listing package to OBS32 Services Branch CM Technical Reference Library (TRL). Once it is logged into the TRL, it is verified by the OBS32 Services Branch CM Analyst.

APPENDIX B. – Radar Operations Center Program Branch Responsibilities

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:

1. Ensure the life-cycle management of WSR-88D System Configuration and its associated technical data package.
2. Ensure the accuracy of the WSR-88D engineering drawings, associated lists, and baseline specifications.
3. 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.
4. 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.
5. Track and facilitate configuration changes through the review cycle.
6. Control the hardware and software product baselines for the system and network.
7. Conduct Configuration Audits to ensure the integrity of the WSR-88D System Baselines.
8. 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.