

State of Maryland NSF Department Change Management Plan (CMP)



Issued on September 9, 2005

**State of Maryland NSF Department
Policy and Procedures Division
2200 Ford Avenue
Laurel, MD 31110
856-679-1650**

TABLE OF CONTENTS

1 INTRODUCTION..... 3

1.1 PURPOSE 3

1.2 SCOPE 3

1.3 APPLICABILITY 3

2 ORGANIZATION AND RESPONSIBILITIES 3

2.1 CHANGE MANAGEMENT PARTICIPANTS 4

2.2 RESPONSIBILITIES 4

3 CHANGE MANAGEMENT PROCESS 6

3.1 ORIGINATION PHASE..... 6

3.2 REQUIREMENTS AND DESIGN PHASE..... 7

3.3 APPROVAL PHASE 8

3.4 DEVELOPMENT PHASE 8

3.5 CLOSURE PHASE 8

4 CHANGE MANAGEMENT SYSTEM 9

5 ADMINISTRATIVE SUPPORT..... 10

APPENDIX B: REQUEST FOR CHANGE (RFC) TEMPLATE 12

APPENDIX C: WORKORDER (WO) RECORD 15



1 Introduction

1.1 Purpose

The purpose of this document is to outline the Change Management Plan that will be put in place. This policy outlines the procedures, policies, and any other document means of accessing the network. Also included are the procedures for updating and maintaining networking equipment.

1.2 Scope

Due to the continuous growth of threats and vulnerabilities, a strong Change Management Plan must be implemented. The State of Maryland's NSF Department's head quarters has outlined the following steps to mitigate the task of proactive updating and upgrading:

- Develop a strong policy with detailed overviews of scope, duties, and implementation planning.
- Educate team members on job duties and reasoning behind continual change management planning.
- Project manager will come up with time frame and formal milestones for initial implementation.
- Security Director will assume responsibility to delegate assessment tasks to subordinates for ensured policy adherence.

The CMP mandates the requirements for procedures and policies related to making changes to the network devices and operating systems.

1.3 Applicability

This plan will be implemented and configured by the State of Maryland NSF Department. The office will also be responsible for maintaining security solutions, procedures and updating polices already in place. This office and the offices under it are responsible for properly maintaining and keeping this management plan in practice.

2 Organization and Responsibilities

Administration

- Approves Change Requests (CR) based on the cost/benefit analysis.

Information Systems

- Creates Change Requests based on un-patched vulnerabilities, bug fixes, service packs, computer/network/infrastructure upgrades and changes.
- Verifies that CRs are aimed at improving Confidentiality, Availability and/or Integrity of the company network infrastructure.

- Tests the configuration change based on the CR.
- Implements CRs after all approvals are made and testing is completed successfully

Procurement

- Approves purchases of hardware/software needed to complete the CR.

Facilities

- Provides preparations for workspace including but not limited to: construction of work areas, utility maintenance, installation of network and/or telephone cables and performing repairs to building and facilities as needed.

2.1 Change Management Participants

The NSF change management process requires the active support and contribution of the NSF responsible organizations:

- The NSF User Group
- The NSF Program Management Office
- The NSF Technical Team
- The Change Management Steering Committee

The NSF Program Management Office serves as the focal point for overseeing the change management process for the company. It is accountable for tracking CRs through the entire cycle from origination to closure to ensure timely and acceptable deliveries to its users. To accomplish this, routine CM changes are to be processed on a continuous basis.

The responsible organizations will be enacting **major changes** by performing the following functions:

- Processing technical change requests via Requests for Change [RFCs] as appropriate
- Providing build management support
- Facilitating communications of changes and impact to the user community and help desk.
- Controlling CM documentation
- Providing CM administration
- Producing CM program metrics.

2.2 Responsibilities

Participant responsibilities are shown below:

The NSF User Group:

- Reflect and represent the interests of the broad cross-section of Agency Users in conducting its work.
- Provide user feedback and functionality requirements, channeling such requirements to the NSF Program Manager for consideration, including:
 - Provide review and a functional requirements statement on all proposed system changes. Through its designated Subject Matter Experts, collaborate with the Technical Team and Program Manager to produce a joint requirements specification.
 - Make recommendations for prioritization of requirements approved by the User Group.
 - Provide user-supported beta testing for new functionality prior to release to production.
 - Provide review and comment to revised User Guides and manuals resultant from enhancements and functionality changes to NSF.

The NSF Program Management Office:

- Perform as the executive agent and Program Manager for NSF.
- Operate as the central focal point for NSF, responsible for its management and budget performance.
- Consider User Group recommendations for NSF.
- Make the formal recommendations on major changes to NSF to the Change Management Steering Committee.

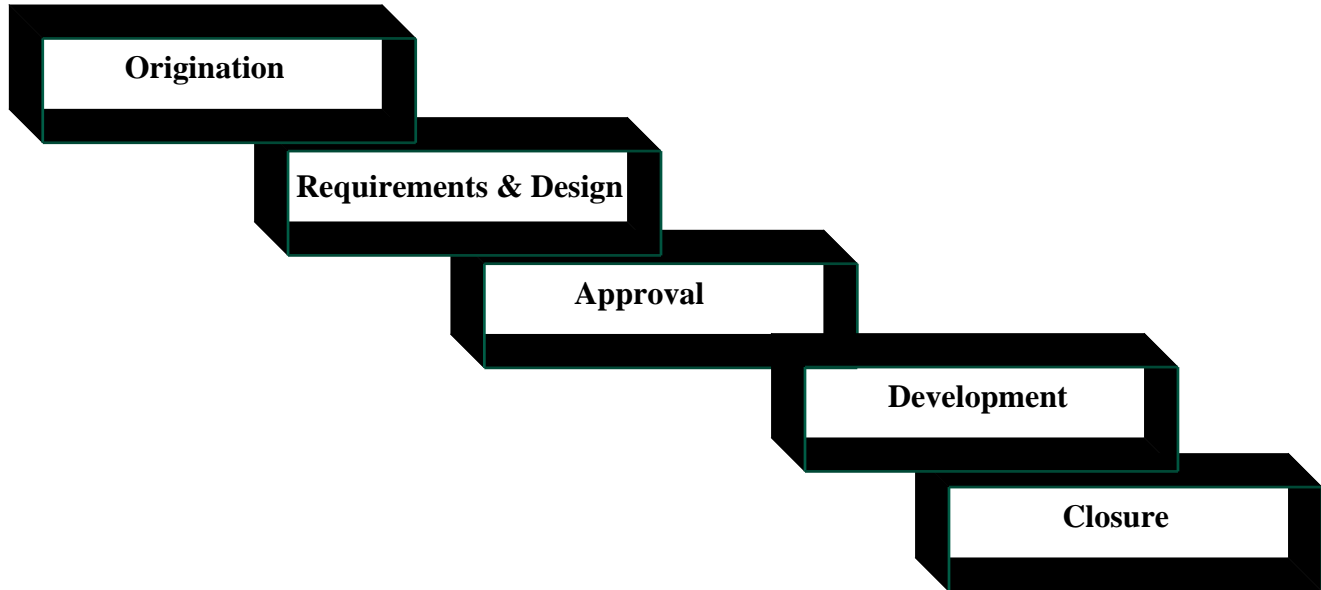
The NSF Technical Team/Manager:

- Perform the day-to-day operational activities of NSF through the Technical Team.
- Provide technical advice to the NSF Program Manager and User Group on proposed changes
- Track CM implementation.

The Change Management Steering Committee:

- Make decisions on major changes to NSF, after reviewing the recommendations of the NSF Program Manager.

3 Change Management Process



**Figure 1: The NSF Changes From Origination Through Review & Approval
To Implementation & Closure**

3.1 *Origination Phase*

3.1.1. Changes

Alterations to Change management Plan regardless of the origination should be submitted through your supervisor. The NSF department will look at the request and forward it to the proper channels. The changes when approved will be made in the order of importance against where they are in the organization.

Issues from the helpdesk are to be classified as Work Orders (WOs see Appendix C), or Requests for Change (RFCs see Appendix B), depending on the scope of the change and whether the request is an actual change or a request to fix a current function of the system.

- A Work Order [WO] is a change that could be an enhancement or a correction but that requires no more than an incidental amount of resources to implement or correct. The Technical Team will resolve the WO and implements the change without involvement by any other CM participant.
- A Request for Change [RFC]:
 - Is requested by the helpdesk (tier 3 support person)

- Changes the functionality of the system
- Involves more than an incidental amount of resources to implement.
- Requires adding to and/or modifying the requirements document.
- Processing
 - RFCs are to be provided to the State of Maryland NSF department for review and processing.
 - The State of Maryland NSF department will review the proposed changes and the impact they will have on security and polices already in place.
 - The standing ISSO at the office the request originated from will also be part of the consideration process and will help determine if it adheres to the plan already in place.

The State of Maryland NSF Security officer (or designee) will be responsible for the final and absolute resolution of a RFC after it has been processed.

3.1.2 Tracking System

The State of Maryland NSF department will maintain the status of RFCs in a statistical database for the monitoring and review of originators and other NSF Change Management participants. Although the WO does not require the comprehensive analysis and development process of an RFC, the WO will also be assigned a number and tracked to closure in the same manner, as RFCs. Once a change request is documented, the submitter will receive notification that their request was received and will be considered and the assigned RFC/WO change management number.

3.2 Requirements and Design Phase

Most changes need to be technically evaluated, prioritized, and estimated in cost/hours, based upon more detailed articulation of the requirement.

A. Detailed Requirements Development:

The NSF Program Management Office will coordinate with the NSF Technical Team and the NSF User Group in the analysis of the RFCs. The NSF Technical Team will coordinate with the NSF User Group's Subject Matter Experts (SMEs), and will facilitate the joint development of a detailed requirements document. Members of the NSF Technical Team and the designated SMEs execute this process. This requirements document should articulate the specific actions taken by the user on NSF as well as the performance or action that results within NSF on a step-by-step basis.

B. Design Phase/Technical Solution Development:

The NSF Technical Team uses the detailed requirements document to formulate a method or methods by which a solution could be implemented to fulfill the requirement. In the case of complex problems, it is often advantageous to have several options available. The estimated cost for implementing the solution package is prepared. While several Technical Team members will contribute, the Lead Developer is responsible for coordinating this task and compiling the proposed solution package.

The NSF Technical Manager will submit the solution package to the NSF Program Management Office. Solution packages are to be periodically grouped into enhancement modules, in approximately six-month intervals. In short, major enhancements will be version-controlled in ordered releases, similar to how commercial software development occurs. The NSF Program Management Office will submit the recommendation to the User Group.

C. User Group Value Decision: The NSF User Group, considering the complete solution package, votes whether to continue supporting the solution based on cost and other factors.

3.3 *Approval Phase*

Before developing the implementation plan, the Security Manager in charge will present the proposed plan before the chosen committee. During this process, the Security Manager should include vital details about the proposed RFC and potential benefits. If a disagreement occurs, plans are then reviewed 30 days after the first attempt. Security Manager in charge of a particular plan must then revise and rework the plan for the second and final selection vote.

Upon approval, the Team will initiate development.

3.4 *Development Phase*

Once approved, the NSF User Group, Program Management Office, and Technical Team work together to develop the approved solution in the Implementation phase. Once a change/proposed solution is approved, it is formally scheduled and assigned.

During development and testing, department heads will be notified by push email of the change and all details that could aid their accommodation to the change for interfacing systems or business practices.

Once the solution is developed, it must undergo testing, including regression testing, prior to release to production. NSF Technical Team personnel will work together to certify that the change does what is intended and that it does not create unintended changes elsewhere in the system. In most cases, NSF Program Management and Technical Team personnel will develop a test plan and one or more test procedures so that the tests are repeatable as more mature versions of the change are developed. Once internal testing is complete, the NSF User Group will be provided with detailed requirements specifications. The NSF User Group will provide User Subject Matter

Experts (SME) (not necessarily the same SMEs as participated in the Requirements and Design Phase), who will test the solution against detailed requirements specifications at a site to be determined by the NSF Technical Team. The SMEs will annotate the results of their testing and will provide the input to the NSF Program Management Office and to the NSF Technical Team. The NSF Technical Team, prior to release, will correct only those issues identified by the SMEs that indicate the detailed requirement has not been met. Issues identified that are “out of scope” of the original requirement will be noted as a potential future enhancement or requirement.

Once the change has been sufficiently tested, the NSF Program Manager signs off on the Build Checksheet. It is then ready to be implemented on the production server.

The NSF Technical Team will post an advance change notification on the NSF home page and by e-mail to users to alert the NSF Headquarters’ user community of the impending changes, the impacts and benefits, system change interface impact, and related instruction in their use. The NSF User Group will be provided the revised NSF User Guide for review and comment.

3.5 Closure Phase

Once the Build Checksheet has been completed, the change is installed. The DR, RFC, or WO that generated the change is updated to reflect the new configuration, and, when all items in the DR, RFC, or WO are to be complete, the document is marked “closed.” If requirements were generated or modified as part of the change, the requirements documentation is edited to reflect the new requirements.

Before implementing the change to the any servers, the technical staff performs all of the items on the Build Checksheet (see appendix A), or confirms that they have been performed. These items include writing release notes, notifying the help desk, detailing user impact (downtime, etc), notifying users of the change and related instructions, testing, installing the build and updates to documentation. The Checksheet is filed with the Deputy Technical Manager once the build is complete.

The RFC, DR, or WO that generated the build is brought up on the CM system and notes are entered as to the solution applied.

The Build Checksheet becomes part of the CM database.

If requirements were created or modified in the course of making the change, the requirements database is modified to reflect those changes along with appropriate adjustments to the State of Maryland NSF Headquarters’ systems and user documentation.

4 Change Management System

The Change Management Plan also includes a planned Change Management System build on a MySQL database and interfaced via a secure intranet web portal. Here, all scanned documents can be tied to a centralized repository and specific reports can be generated. Generated output layouts can be seen in Appendix A and Appendix B for reference. All information on the written forms in Appendix A and Appendix B must be keyed into the system; non-electronic, hand-written copies will not be acceptable.

5 Administrative Support

Administration is needed to support the Change Management Plan. The Security Director plays a crucial role in ensuring proper measures and safeguard are taken in order for proper adherence to this policy and procedure.

Individuals' delegated tasks by the Security Director must adhere to proper procedures and policies. These individuals are overseen by the Security Director and must meet all criteria outlined in this document. If a deficiency is determined, the Security Director has the means to reprimand any individual seen fit for 1.) outages, 2.) improper procedure, 3.) untested upgrades, 4.) unapproved upgrades, and 5.) over-ruling or changing policies and procedures willingly and knowingly.



Appendix A: Build Checksheet

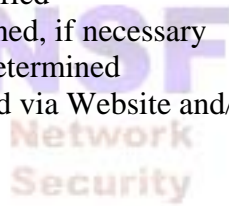
State of Maryland NSF Department

BUILD CHECKSHEET

Circle one: RFC or WO Number: _____

Owner: _____

- _____ Testing is complete and passed
Modules tested: _____
- _____ Release notes have been written and approved
- _____ Build is scheduled
Date: _____
- _____ Outage Message drafted, if necessary
Outage: _____
- _____ Help desk has been notified
- _____ Help desk has been trained, if necessary
- _____ User impact has been determined
- _____ Users have been notified via Website and/or email of impact and outage prior to the build



Build Notes:

When build is complete, submit this sheet to Security Manager.

Appendix B: Request for Change (RFC) Template

ORIGINATOR IDENTIFYING INFORMATION

Name:

Date Prepared:

Agency:

Phone #:

Email Address:

Originator Description of Problem/Request/Requirement:

IDENTIFYING INFORMATION

[Administrative Completion Only Below This Line]

Number:
(Reference Identifier)

RFC-XXXXXX [identifying number]



Title:

Originator Name(s):

Date Prepared:

Projected Implementation Date:

Date Due:

DESCRIPTION OF PROBLEM/REQUEST/REQUIREMENT

Summary of Requested Change:

Scope:

Prerequisites (if any):

Assumptions (if any):

Dependencies / Constraints (if any):

Risks (if any):

Benefits Analysis:

Impact to Users:

Time needed for Preparation:

INVESTIGATOR'S RECOMMENDATION

Comments:

ALTERNATIVE APPROACHES CONSIDERED (optional)

1. Proposed Approach – Option #1

- **Approach overview:**
- **Work Hours (i.e. estimated hours by task):**
- **Material cost in dollars (Hardware/Software):**

Total Hardware and Software Cost:

- **Engineering design concept:**
- **CMP precautions taken to maintain system integrity:**
- **Proposed transition planning:**

- **Implementation schedule with milestone descriptions:**

- **Impact if Option #1 Approach is Approved:**
 - **Development**

 - **O & M**

 - **Training**

 - **Other Program Activities**

 - **Affect on Existing System and Users Including:**
 - **System hardware, software and/or network footprint.**
 - **Facilities and/or equipment.**
 - **User or administrator procedures and processes.**
 - **Operating environment.**
 - **Product form, fit, or functions.**
 - **System performance.**

- **Comment for Option #1:**



Appendix C: Workorder (WO) Record

Requested by:		WO#:	WO-01-NNN
Date:			
Summary:			
Approving Mgr:			
Implemented on:			
Implemented by:			

