Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Standard

Office Instruction:	**CSO-STD-6001**
Office Instruction Title:	**System Change Cybersecurity Significance Standard**
Revision Number:	**2.0**
Effective Date:	**May 31, 2019**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO/CSO**
Description:	CSO-STD-6001, “System Change Cybersecurity Significance Standard,” provides the minimum security requirements that must be met for the cybersecurity significance of a proposed change to an authorized NRC system, including its environment of operation.
Training:	As requested

Approvals			
Primary Office Owner	Office of the Chief Information Officer (OCIO) / Computer Security Organization (CSO)	**Signature**	**Date**
SWG Chair	Bill Bauer	/RA/	4/17/19
CISO	Jonathan Feibus	/RA/	5/23/19

TABLE OF CONTENTS

Computer Security Standard
CSO-STD-6001

System Change Cybersecurity Significance Standard

1 PURPOSE

CSO-STD-6001, "System Change Cybersecurity Significance Standard," provides the minimum security requirements that must be met to ensure a proposed change to an authorized Nuclear Regulatory Commission (NRC) system, including its environment of operation, is awarded the correct level of significance. This standard applies to existing authorized NRC systems processing NRC information up to, and including, the Safeguards Information (SGI) level.

This standard is intended to be used by system owners, enterprise and system-specific Configuration Control Boards (CCBs), Information System Security Officers (ISSOs), Change Coordinators, and system administrators responsible for the security and operations of authorized NRC systems.

This standard is intended to be used in concert with OCIO-CCB-0001, "System Change Significance Determination and Notification Process," and OCIO-CCB-0002, "Change Approval Process."

This standard does ***not*** apply to classified information systems.

2 GENERAL REQUIREMENTS

The significance of changes in the cybersecurity posture of a system or a system's operational environment must be accurately identified. Cybersecurity significance depends on the severity of the change and resulting security impact to a system and/or subsystems.

The two types of changes to NRC information systems, per the Information Technology Infrastructure Library (ITIL) are standard and normal changes.

- Standard Changes: Pre-authorized in accordance with change management processes and have accepted and established procedures to provide specific change requirements. Standard changes follow the NRC CCB process and are not subject to the requirements of this standard. Examples of standard changes include resetting passwords and deployment of security patches within the same major software version.
- Normal Changes: Not pre-authorized, and must follow the complete change management process, including review and approval by the CCB. Normal changes do not always have a known level of security impact. Normal changes are categorized as Minor, Moderate, and Major changes. Examples of normal changes include deployment of new enterprise technologies (e.g., software, hardware, virtual instances).

Emergency, latent, and escalated changes are discussed below in Section 2.2, Changes.

ISSOs must ensure that all implemented changes to a system or subsystem are documented. The documentation within the existing NRC enterprise Information Technology Service Management (ITSM) solution (e.g., BMC Remedy) may be used to satisfy this requirement. System security artifacts (e.g., System Security Plan [SSP], Subsystem Security Plan, and Contingency Plan) should be reviewed and updated to reflect implemented changes, as appropriate. The Change Coordinator (e.g., IT Project Manager, IT System Manager, IT Specialist) must work with the ISSO to ensure that the system change is documented (e.g., in BMC Remedy). ISSOs should make certain that the following is documented, as applicable:

- Date implemented;
- Change description (e.g., a list of firewall rules added, modified, or removed);
- Asset(s)/Asset Group(s) affected; and
- User(s)/User Group(s) affected (if applicable, such as for issuing new equipment).

2.1 Monitoring for and Identification of Changes

Any governing authority, such as ISSOs, system administrators, CCBs, etc., that oversee changes must monitor known changes to a system, as well as the system's environment of operation in order to identify unknown system changes and understand the cybersecurity significance of each change.

2.2 Special Case Changes

There are special case changes encountered in the operational systems environment that include emergency, latent, and escalated changes. These special cases are addressed in the subsections below.

2.2.1 Emergency Changes

An emergency change is a change that must be implemented as soon as possible to resolve a major incident. An emergency change covers the situation where either the impact to service has already been experienced or it is imminent if action is not taken. ISSOs must present the emergency change to the CCB for approval, where going through initial levels of coordination is not required. The alteration to the normal change management process is made to ensure that true emergencies can be responded to in a timely manner, such as a system change to quickly mitigate the identification of a potential or confirmed security breach.

2.2.2 Latent Changes

A latent change is a change that must be implemented immediately to recover from an incident or to resolve a situation where the impact to the service is imminent. A latent change may result from an automated action, such as a server restart initiated by an event monitoring system. When a service provider makes changes to their application or infrastructure that affects agency systems, it is regarded as a latent change. ISSOs, in collaboration with the CCB, must review a latent change after implementation. The latent change should be recorded as it affects services and in some cases, it may have to be rolled back or replaced by another change.

2.2.3 Escalated Changes

An escalated change is a change that must be approved or implemented outside of the normal change management process. An escalated change may result from new requirements in response to implementation of a latent change by a vendor or new requirements imposed by internal or external auditors. An escalated change must be presented to the Chief Information Security Officer (CISO) for approval, instead of going through the CCB approval process due to time constraints. However, the CISO may refer the escalated change to an Authorizing Official (AO) for review and approval, as appropriate.

3 SPECIFIC REQUIREMENTS

The normal change type comprises the following three cybersecurity change categories (also referred to as “cybersecurity significance”):

- Minor, representing the lowest cybersecurity significance
- Moderate
- Major, representing the highest cybersecurity significance

These categories are differentiated between one another with respect to the change severity and level of potential security impact. If more than one cybersecurity significance appears to apply to a change based on the ISSO’s analysis, the ISSO has the right to increase the cybersecurity significance of that change if desired. The subsections below provide the requirements that apply for each category.

The AO or CISO shall have the authority to override the determined cybersecurity significance. If this authority is exercised, supporting rationale should be appropriately documented in the ITSM solution, such as an email attached to the change entry in BMC Remedy.

3.1 Minor Changes (with Minor Cybersecurity Significance)

Minor changes are considered low risk and are typically reoccurring in accordance with existing NRC processes. The applicable CCB, in collaboration with the system ISSO, must determine whether a change can be identified as Minor based upon whether it appears to possess any of the following attributes:

- A change to the system or system’s environment of operation must not present a potential adverse security impact to the system and/or agency.
- A change consists of routine maintenance (e.g., minor software update) or periodic/ad hoc activities that are anticipated (e.g., changing internal firewall rules, building a new server in a test/pre-production environment).
- The change does not result in the addition of new capabilities and functionality for a system.
- The change does not result in non-compliance with any applicable security controls or enhancements for a system (nor for any subsystems).
- The change does not involve the deployment of new devices (e.g., appliances, physical or virtual workstations or servers, network devices) into a production environment.

- The change does not involve the development of new or updating existing custom code (e.g., web, mobile, or native applications).

Based upon operational and cybersecurity expertise within the NRC enterprise and system CCBs, the applicable CCB is permitted the discretion to consider the broader picture of a change's security impact where CCB takes into account provided documentation, such as release notes (e.g., for minor software/firmware updates) for the requested change. The CCB may use this discretion to permit changes to be identified as Minor even if they do not possess all attributes identified above.

In accordance with CCB processes, the CCB is empowered to attach conditions to the recommended approval of Minor changes (e.g., requiring updates on potential security significant portions of a change, further actions, and other follow up).

ISSOs must obtain CCB approval of the proposed Minor change prior to implementation.

3.2 Moderate Changes (with Moderate Cybersecurity Significance)

Moderate changes may affect the security posture of a system. The applicable CCB, in collaboration with the system ISSO, must determine whether a change can be identified as Moderate based upon whether it appears to possess any of the following attributes:

- The change may affect one or more of the following areas of a system that has the potential to present a limited adverse security impact:
  - Cryptographic modules
  - Software installed/in-use on system components
  - Hardware or virtualized system components (e.g., virtual servers)
  - Physical environment and location
  - System functionality and capabilities
  - System access methods
- The change affects the system boundary to add or replace system components, especially in a production role (e.g., new production server).
- Limited change at a subsystem level to enhance the functionality of the overall system (e.g., addition of a new virtualized pre-production environment for an NRC infrastructure system).
- The change may not present a new High risk to the system or agency.
  - CCBs have the ability to approve Moderate changes that contain High risks that are already open and identified (e.g., within prior security assessments and in the Plan of Action & Milestones [POA&M]) for the system. This is typically identified by review of current system or agency level POA&M.
  - CCBs shall not approve Moderate changes that contain one or more High risks that are not currently open and identified for the system. A change with one or more High risks of this type is considered a Major change (refer to Section 3.3, Major Changes (with Major Cybersecurity Significance), for details).

Based upon the operational and cybersecurity expertise that is possessed by the NRC enterprise and system CCBs, the applicable CCB is permitted the discretion to consider the broader picture of a change's security impact. The CCB may use this discretion to permit changes to be identified as Moderate even if they do not possess all attributes identified above.

In accordance with CCB processes, the CCB is empowered to attach conditions to the recommended approval of Moderate changes (e.g., follow-up security assessments, targeted analysis following implementation, updates on security finding remediation).

ISSOs must ensure that a security assessment of a proposed Moderate change is performed and obtain CCB approval prior to implementation. ISSOs should identify and document the affected security controls as part of the change request, as appropriate.

3.3 Major Changes (with Major Cybersecurity Significance)

A Major change carries the potential for a large adverse security impact. Major changes can involve a significant amount of preparation and work with complex situations at a considerable expense. For example, when a change alters key characteristics of the system, such as the security categorization, system boundary, and infrastructure, it is regarded as a Major change.

The CCB, in collaboration with the system ISSO, must determine whether a change can be identified as Major based upon whether it appears to possess any of the following attributes:

- A change that can be expected to present significant increased risk to a system which exceeds the level of risk accepted on behalf of the agency by the AO as part of system authorization. A newly identified High risk would be an example, as it does not already exist within the system.
- A change that does not comply with the system authorization conditions.
- A change that affects the security categorization level of a system.
- A change that involves the use of new public, private, or hybrid cloud or external (e.g., hosted by another federal agency) computing services that are not authorized by the AO.
- A change that involves transitioning a system that is hosted internally within the NRC or by a contractor specifically for NRC to a cloud or external service provider.
- A change that involves expanding a system boundary to include one or more additional system or subsystem or removal of such subsystem which affects the system boundary.
- A change to the system infrastructure, architecture, and connectivity (e.g., virtualizing the entire network infrastructure for a system).
- A change to introduce a new technology to the agency, such as a new operating system, that is anticipated to be used across the enterprise that has the potential for a large adverse security impact.
- A change to add a new facility or data center to expand the existing system.
- A change to add a pilot system for a proof-of-concept or an addition/replacement to the existing system (e.g., transition to cloud services).

ISSOs must ensure that Major changes are approved by the CISO or AO. The CISO will have the ability to determine if AO authorization is needed (e.g., authorization of a Federal Risk and

Authorization Management Program [FedRAMP] new cloud service provider). The CISO or AO may also approve Major changes with specific conditions (e.g., regarding remediation of identified findings).

In accordance with CCB processes, the CCB is empowered to propose conditions to the recommended approval of Major changes (e.g., follow-up security assessments, targeted analysis following implementation, updates on security finding remediation) to the CISO or AO.

ISSOs must ensure that an independent security assessment of the proposed Major change is performed in accordance with Computer Security Organization (CSO) processes, in collaboration with the CSO point of contact for the system, and in accordance with the direction of the CISO and AO.

If the Major change affects other systems or subsystems, the ISSO must inform the other relevant ISSOs and should consider informing relevant system owners, where appropriate.

APPENDIX A. ACRONYMS

AO	Authorizing Official
CCB	Configuration Control Board
CISO	Chief Information Security Officer
CIO	Chief Information Officer
CSO	Computer Security Organization
FedRAMP	Federal Risk and Authorization Management Program
ISSO	Information System Security Officer
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITSM	Information Technology Service Management
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
POA&M	Plan of Action & Milestones
SGI	Safeguards Information
SSP	System Security Plan

APPENDIX B. GLOSSARY

Authorizing Official	An official, such as the Chief Information Officer (CIO), who has ultimate authority to make decisions on matters related to agency information systems.
Change Coordinator	A coordinator, such as IT Manager or IT Specialist, is responsible for the quality and integrity of a change management process impacting a specific project or a system.
Cloud Service Provider	A company that offers some component of cloud computing as a service to other businesses or agencies.
Emergency Change	A change that must be implemented immediately to resolve a major incident or implement a critical security patch to avert a security breach, for example. This change does not follow the normal change management process but requires CCB approval.
Escalated Change	A change that must be approved or implemented outside of the normal change management process, possibly resulting from the implementation of other immediate changes (i.e., latent changes). An escalated change is approved by the CISO due to time constraints.
External Service Provider	A legally independent enterprise that performs work based on the contract for a business or an agency.
Latent Change	A change that must be implemented immediately to combat a major incident or a security breach without following the normal change management process, but requires CISO or AO approval.
Major Change	A change to a system or the environment of operations for a system that affects the security posture and can be expected to present the greatest potential adverse security impact to the system and/or agency (when compared to Moderate and Minor changes).
Minor Change	A change to a system or the environment of operations for a system that could be expected to present little or no adverse security impact to the system and/or agency.
Moderate Change	A change to a system or the environment of operations for a system that affects the security posture and can be expected to present a limited potential adverse security impact to the system and/or agency.
Normal Change	A change that must follow a change management process and is categorized according to the risk and impact to the agency.
Safeguards Information	A special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act to be protected.

Standard Change	A change to the infrastructure for which the approach is pre-authorized by change management that has an accepted and established process to provide a specific change requirement.
System Change Cybersecurity Significance	The level of cybersecurity significance of a proposed change to an authorized NRC system, including its environment of operation. Also referred to as cybersecurity significance.

CSO-STD-6001 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
4-Feb-16	1.0	Initial Issuance	Distribution at ISSO forum and posting on ISD web page	Upon request
23-May-19	2.0	Updated with latest requirements	Post to OCIO/CSO web page	Upon request