NSCS Information Security Standard 7: Configuration and Change Management

7.1 Configuration Management

- Technology Resources may be assigned different change control processes based on the classification level identified in Information Security Standard 4.1.
- Baseline configurations or standard configurations will be maintained at the discretion of the CISO with an emphasis on systems processing medium and high risk data. See Information Security Standard 6: *Computer and Network Security* for minimum requirements for standard configurations.
- A basic network diagram must be maintained on an annual basis.
- NSCS owned or issued computer or related equipment (e.g., servers, workstations, laptops, PDAs, printers, fax, and other such devices) that can be connected to an NSCS network, or used to capture, process or store NSCS data, or used in the conduct of NSCS business should be tracked in an inventory tracking system that identifies (at a minimum) its serial number, location, classification level (if assigned), and assigned responsible employee.
- Capitalized equipment with inventory tags must be reported to the applicable inventory management office.

7.2 Change Management

The goals for the NSCS IT Change Management Program are:

- The NSCS recognizes the ITIL definition of change and levels of change:
    - Change - The addition, modification or removal of anything that may have an impact on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items.
    - Types of Change
        - Standard - A pre-authorized change that is low risk, relatively common and follows a documented procedure or work instruction. Standard changes need not be tracked, approved, or documented.
        - Normal - Any service change that is not a standard change or an emergency change.
        - Emergency - A change that must be implemented as soon as possible, for example to resolve a major incident or implement a security patch.
- All Normal changes should be documented, scheduled and tracked within the applicable Information Technology department. Automated tracking systems are preferred.
- Change records are to provide enough detail to accurately document the changes being made.
- Changes may only be implemented once the change record has been approved.

- Changes may be approved by a workflow that follows College procedures for the change level indicated.
- Emergency changes may go through an expedited review and approval process but should always go through a formal review process afterwards.
- The status of changes that did not go as planned, or that did not have the expected results, will be reviewed for completeness and impact to the IT. The change implementer is required to participate.

Revision History

April/14/2019: Initial submission by PCSS
May/8/2019: Initial review by SOISO/CISOs
July/8/2019: Second review by SOISO/CISOs
July/26/2019: Third review by SOISO
Oct/1/2019: Fourth review by SOISO