	Department of Human Services Online Directives Information System	Index: Revised: Next Review:	POL1903 06/03/2019 06/03/2021

SUBJECT: DHS Information Security Policies

Configuration Management Policy

POLICY

This policy establishes the Enterprise Configuration Management Policy, for managing risks from system changes impacting baseline configuration settings, system configuration and security. The configuration management program helps DHS document, authorize, manage and control system changes impacting Information Systems.

Authority

1. United States Department of Commerce National Institute for Standards and Technology (NIST)
2. United States Internal Revenue Service
3. United States Department of Health & Human Services
4. Centers for Medicare & Medicaid Services
5. Georgia Technology Authority

References

- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4, January 2015
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-128 “Guide for Security Configuration Management of Information Systems” August 2011
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-70 “National Checklist Program for IT Products – Guidelines for Checklist Users and Developers” Revision 4 February 2018
- United States Department of Commerce National Institute for Standards and Technology (NIST) Special Publication 800-60 “Guide for Mapping Types of Information and Information Systems to Security Categories” Volume 2 Revision 1 August 2008
- United States Internal Revenue Service, IRS Publication 1075 Tax Information Security Guidelines For Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information
- Centers for Medicare & Medicaid Services, Volume II: Minimum Acceptable Risk Standards for Exchanges

Applicability
The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by DHS. Any information not specifically identified as the property of other parties, that is transmitted or stored on DHS IT resources (including e-mail, messages and files) is the property of DHS. All users (DHS employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

Definitions
None

Responsibilities
DHS shall adopt the Configuration Management principles established in NIST SP 800-53 "Configuration Management," Control Family guidelines, as the official policy for this domain. The following subsections outline the Configuration Management standards that constitute DHS policy. Each DHS Business System is then bound to this policy, and shall develop or adhere to a program plan which demonstrates compliance with the policy related the standards documented.

- **CM-1 Configuration Management Policy and Procedures**
    1. Senior management, management, and all organization entities are required to coordinate and implement necessary controls for implementing configuration management of IT resources and information systems on the basis of business and security requirements.
    2. Periodic reviews of this access control policy shall be performed and documented at least within every **three years**, or when there is a **significant change**.
    3. Periodic review of configuration management procedures shall be performed at least **annually**.
- **CM-2 Baseline Configuration**
    1. Current baseline configurations for DHS information systems is developed, documented and securely maintained. Baseline configurations shall be reviewed and updated:
        a) At a minimum **annually**.
        b) When required due to system upgrades, patches, or other significant changes.
        c) As an integral part of information system component installations and upgrades.
    2. The baseline configuration must include documented, up-to-date specifications to which the information system is built and configured.
    3. The baseline configuration must document and provide information about the components of an information system including:
        a) Standard operating system/installed applications with current version numbers

b) Standard software load for workstations, servers, network components, and mobile devices and laptops
c) Up-to-date patch level information
d) Network topology
e) Logical placement of the component within the system and enterprise architecture
f) Technology platform

4. New baselines must be created as the information system changes over time as this includes maintaining the baseline configuration.
5. The baseline configuration of the information system must be consistent with DHS' enterprise architecture.
6. The DHS-defined list of software programs authorized to execute on the information system is currently developed and maintained.

- **CM-3 Configuration Change Control**

Change control management is required for key information systems. The following applies to all agency systems which must enter the configuration change control process:

1. The types of changes to the information system that are to be configuration-controlled must be determined.
2. All changes to the information system that are determined to be configuration-controlled must be approved and documented.
3. The approvals to implement a configuration-controlled change to the information system must include explicit consideration for the security impact analysis.
4. Records of configuration-controlled changes to the system must be retained and reviewed.
5. Implement approved configuration-controlled changes to the information system for the life of the system.
6. Retaining and reviewing records of configuration-controlled changes to the information system.
7. Oversight for configuration change control activities must be provided and coordinated through DHS' Change Advisory Board (CAB) that convenes at least once per month.
8. Configuration change control must include changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers).
    i. Emergency changes, including changes resulting from the remediation of flaws, must be included in the configuration change control process
9. Changes to the information system must be tested, validated, and documented before implementing the changes on the operational system.
    i. Testing must not interfere with information system operations.
    ii. The individual/group conducting the tests must understand DHS'

information security policies and procedures, the information system security procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process.

- **CM-4 Security Impact Analysis**
    1. Prior to change implementation, changes to the information system must be analyzed to determine potential security impacts.
    2. Security impact analyses must be conducted by organizational personnel with information security responsibilities, including for example, Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers.
        a) Individuals conducting security impact analyses must have the appropriate skills and technical expertise to analyze the changes to information system and the associated security ramifications.
        b) The security impact analysis must be provided to the Chief Information Security Officer (CISO) upon request to ensure that the CISO is aware of any changes to the security controls which may impact the security posture of the information system.
    3. The security impact analysis must include, but is not limited to:
        a) Reviewing information system documentation to understand how specific security controls are implemented within the system and how changes might affect the controls.
        b) Assessing risk to understand the impact of the changes and to determine if additional security controls are required.
    4. The security impact analysis must be scaled in accordance with the security categorization of the information system.
    5. The baseline configuration and system components inventory, as defined in CM-2 and CM-8, must be changed only through an approved change control process.
- **CM-5 Access Restrictions for Change**
    1. Physical and logical access restrictions are defined, documented, approved by management, and enforced with changes to the information system.
    2. Individuals authorized to perform configuration changes must be documented.
    3. Only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.
    4. Access records must be maintained to ensure that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system.
- **CM-6 Configuration Settings**

1. Mandatory configuration settings for information technology products must be established for the information system using a security configuration checklist that reflect the most restrictive mode consistent with operational requirements.
2. Configuration settings must be implemented and exceptions from the mandatory configuration settings must be identified, documented, and approved for individual components within the information system based on explicit operational requirements.
3. Deviations from established configuration settings for information systems that receive, process, store, or transmit FTI, are identified, documented, and must be approved by management prior to implementation.
4. Control changes to the configuration settings are implemented in accordance with agency established policies and procedures.

- **CM-7 Least Functionality**
  1. The information system must be configured to provide only essential capabilities.
  2. Agency information systems are prohibited from utilizing functions, ports, protocols, and/or services as defined in, but not limited to, the Office of Safeguards- approved compliance requirements.
  3. As a party of agency vulnerability assessments, information systems are review to identify and disable unnecessary or non-secure functions, ports, protocols, and services.
- **CM-8 Information System Component Inventory**
  1. DHS contracted service provider maintains an inventory of the information system components which:
     a) Accurately reflects the current information system within the agency's enterprise.
     b) Includes all components that store, process, or transmit FTI.
     c) Provides the requirements necessary for tracking and reporting agency information system inventory information
     d) Includes information deemed necessary to achieve effective information system component accountability.
  2. The inventory of information system components must include any information determined to be necessary by the organization to achieve effective property accountability including, but not limited to:
     a) Manufacturer
     b) Type
     c) Model
     d) Serial number
     e) Physical location
     f) Software license information
     g) Information system/component owner
     h) Associated component configuration standard
     i) Software/firmware version information

j) Networked component/device machine name or network address

3. The information system component inventory is updated and maintained for accuracy through periodic manual inventory checks.
4. The inventory of information system components is regularly updated as component installations, removals, and information system updates are performed.

- **CM-9 Configuration Management Plan**
  1. DHS contracted service providers have developed, documented, and implemented a configuration management plan for the agency's information system which identifies roles, responsibilities, and configuration management processes and procedures.
  2. Configuration items are defined and identified throughout the System Development Life Cycle (SDLC) for agency information system and implemented via documented configuration management processes.
  3. The configuration management plan is accessible only to authorized personnel, and is protected from unauthorized disclosure and modification via implemented access controls.

- **CM-10 Software Usage Restrictions**
  a) DHS enforces the appropriate use of software and associated documentation to ensure utilization of software in accordance with contract agreements and copyright laws.
  b) Software and associated documentation is tracked via software inventory, and is protected by tracking quantity licenses to control copying and distribution.
  c) Peer-to-peer file sharing is restricted to specific roles which are required for identified business processes. Only authorized personnel and user roles shall have utilize peer-to-peer file sharing for the purpose of performing agency identified business functions. The use of peer-to-peer file sharing is documented and controlled to ensure that it is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work.
  d) The installation of Open Source Software is restricted to software which must:
    i. Be legally licensed
    ii. Be approved by the DHS Office Of Information Technology
    iii. Adhere to the secure configuration baseline checklist from the U.S. Government, agency, or industry.

- **CM-11 User Installed Software**
  1. Users are prohibited from installing unauthorized software.

2. Users must request a waiver from the Georgia Technology Authority (GTA) if user installed software is required to perform necessary business functions. All requirements for the GTA waiver must be met and the waiver approved prior to installation of the user installed software.
3. Software installation policies are enforced through automated methods (i.e. automated configuration setting implementation and maintenance). Additionally:
    a) Software lists are reviewed semi-annually.
    b) Agency system administrators are notified if unauthorized software is detected on agency information systems. Administrators must remove software immediately and document the infraction.
4. Policy compliance is monitored on a **continual basis**.

History

None