Chapter 124

Title: DHS Information Systems Change Management Procedures

I. Applicability

These procedures apply to all employees and authorized users who install, operate, or maintain DHS information resources.

II. Scope

This procedure ensures that changes to information systems are deployed in a controlled manner so that DHS users and clients can plan accordingly. Changes require careful evaluation, prioritization, planning, testing, implementation and documentation to reduce negative impact to DHS' business and user community. Management of these changes is a critical part of providing strong and valuable information systems throughout the agency.

III. Procedures

(a) All changes to the DHS information systems or resources shall comply with this procedure.

(b) All changes affecting DHS' computing environmental facilities (for example, air conditioning, water, heat, plumbing, electricity, and alarms) need to be reported and coordinated with the DHS Chief Information Officer (CIO) or Chief Information Security Officer (CISO). These changes shall adhere to any applicable state regulations.

(c) All change requests must be submitted in writing to the CIO or desingee by the end of business on Wednesday to be reviewed by the DHS Change Management Committee on Friday.

(d) The members of the DHS Change Management Committee meets with the appropriate agency systems managers to review, assess, and evaluate all change requests.

(e) If the proposed change is authorized, the committee plans the update and coordinates the implementation of the change, then after the final review, the change process is closed.

(f) The CIO or CISO and the DHS Change Management Committee may deny the standard change or an emergency change for the following reasons:

(1) Planning (for example, inadequate planning related to implementation, risk assessment, testing, back-out);

(2) Timing (for example, timing of a change that would negatively impact a key business process such as year-end accounting);

(3) Documentation (for example, inadequate documentation related to disaster recovery, security testing methodology/data); or

(4) Resources (for example, adequate resources may particularly be a problem on weekends, holidays, or during special events).

(g) DHS user notification (located on the DHS Sharepoint site) must be completed for each Standard and Emergency Change by utilizing these procedures included in this section.

(h) A Change Management log must be maintained for all changes. The log must contain, but is not limited to:

(1) Date of submission and date of Change;

(2) Owner and custodian contact information;

(3) Nature of the Change; and,

(4) Indication of success or failure.

(i) A change review must be completed and documented for all changes, whether the change is successful or not.

(j) All DHS Information Systems, network devices, and databases will use approved baseline configurations and hardening per the DHS Configuration Standards and National Institute of Standards Technology guidelines. Any deviation from the standard baseline configuration must be approved by the CIO or CISO prior to implementation.

(k) The DHS IT Security Office ensures that DHS maintains information and system integrity through intrusion detection systems that facilitate notification of unauthorized changes.

IV. Failure to Comply

Failure to comply with this procedure may result in restriction or suspension of all access to DHS information systems. Employees who can't complete job duties or assignments without such access can be terminated or face disciplinary action as outlined in DHS Policies 4002, "Privacy and Security Sanctions" and 1084, "Employee Discipline: Conduct/Performance."

V. Definitions

(a) "Back-out Plan" means a plan that documents all actions to be taken to restore a service or service component if the associated Change or Release fails or partially fails. Back-out plans may provide for a full or partial reversal.

(b) "Change" means the addition, modification or removal of an authorized, planned or supported service or service component and its associated documentation. All Changes must be registered by the Change Management process.

(c) "Emergency Change**"** means an authorized modification that is intended to repair a failure in an Information Technology service that may have a significant negative impact on DHS business.

(d) "Standard Change**"** means an authorized, planned modification or upgrade of a service or infrastructure component that is of low risk.

(e) "Change Management" means the process responsible for the lifecycle of all Changes. The primary objective of Change Management is to enable beneficial changes to be made, with minimum disruption to DHS Information Systems. The process includes the management and coordination of the processes, systems and functions required for the packaging, building, testing and deployment of a release into production, and establish the service specified in the customer and stakeholder requirements.

(f) **"**DHS Information Systems" means the DHS Network services (Network access, Email, Internet, etc.), DHS applications (client-server, web-based, mainframe, etc.), or any third-party software legally acquired and installed on the DHS device for which they were intended. A DHS Information System also includes any computer file, on any device in use by DHS or its agents, that is shared across the DHS network or that requires DHS support or that contains DHS-related information, the privacy of which must be safeguarded.

(g) "DHS User" means a person whose identity has been validated, whose association with DHS has been certified by the division with whom the person is affiliated, who has been granted access to any DHS Information Systems, and who is held accountable for the security of such access. A DHS User may or may not be a DHS employee.

(h) "Information Resources" means any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving e-mail, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistant (PDA) devices, pagers, distributed processing systems, telecommunication resources, network environments, telephones, fax machines, and printers. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

(i) "Release" means a collection of hardware, software, documentation, processes or other components required to implement one or more approved Changes to DHS Information Services. The contents of each Release are managed, tested, and deployed as a single entity.

(j) "Request for Change (RFC)" means a formal proposal for a change to be made. A Request for Change includes details of the proposed change.

(k) "DHS System Manager" means the persons exercising management authority for a DHS-supported network service or application system. The role of such persons provides DHS ownership for the DHS service or system.

VI. References:

(a) Arkansas Physical and Logical Security Standard for Information Technology Resources (SS-70-008) http://www.dis.arkansas.gov/policiesStandards/Documents/SS-70-008_phys_log_standard.pdf

(b) Arkansas Physical and Logical Security Standard Guidelines Document Number SS-70-008 http://www.dis.arkansas.gov/poli_stan_bestpract/pdf/PhyLogGuidelines.pdf

(c) Health Insurance Portability and Accountability Act of 1996 (HIPAA) http://www.hhs.gov/ocr/privacy And Patient Protection and Affordable Care Act of 2010

(d) Information Technology Infrastructure Library version 3 (ITIL v3) http://www.itil-officialsite.com/home/home.asp

(e) Copyright Act of 1976; U.S. Copyright Law of 2007; Enactments to amend U.S. Copyright Law, 2008; http://www.copyright.gov/title17

(f) Foreign Corrupt Practices Act of 1977, as amended http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/47mcrm.htm

(g) Computer Fraud and Abuse Act of 1986 http://www.justice.gov/criminal/cybercrime/1030_new.html

(h) Computer Security Act of 1987 http://www.csp.noaa.gov/policies/csa-1987.htm

(i) Critical infrastructure Executive Order 13636

(j) IRS Publication 1075

(k) Federal Information Security Management Act of 2002

(l) The Health Information Technology for Economic and Clinical Health Act of 2009

(m) The Privacy Act of 1974

(n) Act 339 of 2007, State of Arkansas, PIPA, ACA 4-110-104

(o) The e-Government Act of 2002

(p) HHS Final Rule 155.260 Privacy and Security of Personally Identifiable Information

(q) 26 U.S.C. §6103 Safeguards for Protecting Federal Tax Returns and Return Information

(r) USA Patriot Act of 2001, USA Cyber Security Enhancement Act of 2002, USA Computer Fraud and Abuse Act of 1986

(s) 18 U.S.C. § 1029. (Fraud and Related Activity in Connection with Access Devices); 18 U.S.C. § 1030. (Fraud and Related Activity in Connection with Computers); and 18 U.S.C. § 1362. (Communication Interference)