5010 Division and Office IT Security Requirements

I. Applicability

All DHS Divisions and Offices and IT staff must follow the security rules prescribed here as they are mandated by various state and federal regulations. All DHS IT security policies (5000 series) and procedures (APMs 120-129) must be followed so that the agency remains in compliance with all state and federal laws.

II. Privacy and Security Incident Response

(a) The IT Security and Privacy Offices will conduct investigations, determine the severity of each incident, and assist Divisions in staying in compliance with all applicable federal and state laws.

(b) The IT Security Office or the Privacy Office (within OPLS) shall:

(1) inform DHS executive staff of privacy or security vulnerabilities and incidents that threaten the confidentiality, integrity or availability of DHS information, network, or systems and provide strategies to mitigate the identified risks;

(2) provide quick, effective, and orderly responses to privacy or security related incidents;

(3) facilitate privacy or security related process improvement activities and create or modify policy to better to reduce the risk of future incidents;

(4) document incidents, maintain incident activity logs for quarterly review, and preserve evidence collected during the investigation;

(5) maintain incident response handling procedures regarding notification, assessment, investigation, remediation, monitoring, and final reporting of incidents; and,

(6) maintain procedures to report criminally related privacy or security incidents to outside authorities in compliance with appropriate legal requirements and regulations.

(c) Notifications for victims of breaches of protected information will be determined by the Privacy Officer who will strictly follow the regulations established by all applicable state and federal regulations.

(d) The Chief Information Security Officer (CISO) and IT Security Office are responsible for determining the necessary steps for containment, tracing, and analysis and will work with the DHS Chief Information Officer (CIO) to reduce the impact within the divisions.

(e) Notifications for the general public will be determined by federal and state regulations and involve the CIO, CISO, Privacy Officer, OPLS Director, and the DHS Director's Office.

III. Security Planning

All divisions and offices must adhere to the Office of Systems & Technology's (OST) IT Security Plan. Division and Office IT Managers may consult with the Chief Information Security Officer (CISO) or the DHS IT Security Office for more information on the Security Plan.

IV. Acquisitions and Systems Integration

(a) All acquisitions of information systems technology or services (hardware, communications equipment, professional services, open market software acquisitions, etc.) must be coordinated with and approved by the DHS Chief Information Officer (CIO) and follow the procedures as outlined in "Information Systems Development & Acquisition Procedures" (APM 122).

(b) All DHS project managers and application owners will work with the IT Security Office and the DHS Privacy Office during the planning, purchasing, and development phases of IT acquisitions to ensure compliance with DHS policy and state and federal laws.

(c) To ensure the security and integrity of DHS data, all software purchased or used within DHS systems shall be within current version and 2 revisions and updated as released. This includes supporting software such as Java, Silverlight, and web browsers.

(d) The DHS CIO must approve all protected data integration with the system to ensure the confidentiality and integrity of the data and network. Integration of any hardware, software, or peripheral with DHS information systems shall be approved in writing by the CIO prior to integration. Requests for integration should be submitted to the DHS CISO with sufficient time for review prior to integration.

(e) Any service agreements with outside vendors and contractors that may require the release of protected health information requires the approval of the DHS Privacy Officer prior to activation.

V. Risk Assessments

(a) Risk assessments can be conducted on any DHS division or office and any outside entity that has a signed contract or Business Associate Agreement (BAA) with DHS.

(b) Risk assessments can be conducted on any information system (including applications, servers, and networks) and any processes or procedures used in

administering or maintaining these systems. Individuals must fully cooperate with any risk assessments being conducted on systems for which they are held accountable.

(c) The execution, development, and implementation of any remediation program put in place after a risk assessment is the responsibility of the CISO, Privacy Officer, and the division or office responsible for the system being assessed.

VI. Data Classification

(a) All DHS data is evaluated, properly classified, and labeled so that the appropriate access controls are implemented to protect that data. DHS Divisions/Offices shall implement the appropriate safeguards based on the confidentiality level of the data to include Unrestricted, Sensitive and Confidential Information using the "Data Classification Procedure" (APM 123).

(b) Each DHS Division/Office shall utilize more stringent security control requirements when the Security Level of an information system, facility, or network is designated at the "Sensitive" or "Confidential" level. In all instances, the minimum security requirements of a system should be appropriate for the highest security level designation of any data the DHS Division/Office processes within that system, including data received from other agencies.

(c) All DHS Applications/Systems shall implement the appropriate security controls to minimize risk in the production or operating environment. The type of controls necessary will be commensurate with the determination of data confidentiality, integrity, and availability levels. The DHS CIO shall certify the controls as appropriate based on classification of the data or system.

VII. Data Encryption

All DHS data encryption must follow the "Acceptable Encryption Procedures" (APM 126).

VIII. Security Emergency Management

(a) DHS Divisions will assign a Disaster Recovery (DR) Manager. The IT Disaster Recovery Manager is responsible for overseeing IT DR activities, for their divisions, in the event of an emergency, for example, an unplanned outage where Real Time Operations are in jeopardy. The IT Disaster Recovery Manager should be part of the IT representation within the institution's Emergency Management Team.

(b) Each division must develop and maintain a documented emergency plan including notification procedures.

(c) Each division shall account for its associates when a building evacuation is ordered. Supervisory personnel are responsible to account for the associates they supervise.

(d) The IT Disaster Recovery Team/Manager is required to complete a post-mortem report documenting outages and recovery responses within 45 days after the occurrence of a disaster recovery event.

(e) For further planning and how to respond to IT Security Emergencies, each Disaster Recovery Manager and DHS Divisions and Offices must follow "Information Systems Disaster Recovery and Continuity Procedures" (APM 128).

IX. Failure to Comply

Violations of this or any DHS Privacy or Security Policy or procedure may result in disciplinary action as outlined in DHS Policies 4002, "Privacy and Security Sanctions" and 1084, "Employee Discipline: Conduct/Performance."