DOJ 2640.2F

INFORMATION TECHNOLOGY SECURITY

Approval Date: November 26, 2008

Approved By: LEE J. LOFTHUS
Assistant Attorney General for Administration

Distribution: BUR/H-1; OBD/H-1; SPL-23

Initiated By: Department Chief Information Officer

FOREWORD

1. **PURPOSE.** This order establishes uniform policy, responsibilities and authorities for protection of Information Technology (IT) systems that store, process or transmit Department of Justice (Department) information.

2. **SCOPE.** The provisions of this order apply to all Department Components, personnel and IT systems used to process, store or transmit Department information. They apply to contractors and other users of IT systems supporting the operations and assets of the Department, including any non-Department organizations and their representatives who are granted access to Department IT resources, such as other Federal agencies. This policy applies to IT systems processing National Security Information and unclassified information.

3. **CANCELLATION.** Department Order 2640.2E is cancelled.

4. **AUTHORITIES.** The Department Chief Information Officer (CIO) is responsible for providing policy, guidance, implementation and oversight for IT systems.

5. **REPERCUSSIONS FOR COMPONENT NON-COMPLIANCE.** The Department CIO may take appropriate action if a Component, contractor or other non-Department organization or their representatives are found to be non-compliant with Department IT security policy. The Department Chief Information Security Officer (CISO), and Department Security Officer (DSO) shall be notified in cases of such non-compliance in order to take appropriate action.

6. **REFERENCES.** References to various regulations and laws applicable to the responsibilities of IT security are located in APPENDIX 1. Future updates to referenced documents will be considered applicable to this order.

7. **DEFINITION OF TERMS.** Terms shall have the meaning defined by National Institute of Standards and Technology Interagency Reports (NISTIRs), Federal Information Processing Standards (FIPS) and Special Publications (SP). Unless otherwise stated, all terms used in NIST publications are also consistent with the definitions contained in the Committee on National Security Systems Instruction No. 4009, National Information Assurance Glossary.

/s/LEE J. LOFTHUS
Assistant Attorney General
for Administration

TABLE OF CONTENTS

CHAPTER 1. INFORMATION TECHNOLOGY SECURITY POLICY

1. Component Information Technology Security Programs.

Each Component shall establish and maintain an IT security program, in compliance with the Department's overall IT security program, to ensure the confidentiality, integrity and availability of the Component's computer systems, networks and data, in accordance with all Federal and Department policies, standards, procedures and guidance.

2. Required Use of DOJ IT Systems

DOJ information used for official business may only be processed, stored, or transmitted on IT systems meeting the requirements of this order.

This restriction does not apply to DOJ information disseminated to other Federal, State, Local or Tribal agencies, or to information released to the public or as part of a court proceeding, or to information whose release is required to accomplish a non-DOJ function (e.g., information released to a hospital so it can provide health care services to a prisoner).

3. Management Security Policy

a. **Risk Assessment**. In accordance with DOJ IT Security Standard - Risk Assessment (RA) Control Family, Components shall periodically assess the risk to Departmental operations (including mission, function, image or reputation) and assets, individuals, other organizations, and the Nation resulting from the operation of Department IT systems and the associated processing, storage, or transmission of Department information.

b. **Planning.** In accordance with DOJ IT Security Standard – Planning (PL) Control Family, Components shall develop, document, periodically update and implement security plans for Department IT systems that describe the security controls in place or planned for the IT systems and the rules of behavior for individuals accessing the IT systems.

c. **System and Services Acquisition.** In accordance with DOJ IT Security Standard – System and Services Acquisition (SA) Control Family, Components shall:

(1) Allocate sufficient resources to adequately protect Department IT systems.

(2) Employ systems development life cycle processes that incorporate IT security considerations.

(3) Ensure new acquisitions include available Commonly Accepted Security Configurations.

(4) Perform acquisition risk assessments, and develop and adopt effective supply chain risk mitigation for IT acquisitions.

(5) Employ software usage and installation restrictions to ensure software installed on Component IT systems is in compliance with applicable copyright laws and licensing agreements.

(6) Ensure third-party providers are contractually required to comply with this policy to employ adequate security measures to protect information, applications and/or services outsourced from the Department.

d. **Certification, Accreditation and Security Assessments.** In accordance with DOJ IT Security Standard – Certification, Accreditation and Security Assessments (CA) Control Family, Components shall:

(1) Periodically assess the security controls in Component IT systems to determine if the controls are effective in their application.

(2) Develop, monitor and implement plans of action and milestones (POA&M) designed to correct deficiencies and reduce or eliminate vulnerabilities in Component IT systems.

(3) Authorize the operation of Component IT systems and any associated IT system interconnections prior to operational use, and notify the Component CIO.

(4) Monitor IT system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

4. Operational Security Policy

a. **Personnel Security.** In accordance with DOJ IT Security Standard – Personnel Security (PS) Control Family, Components shall:

(1) Ensure individuals occupying positions of responsibility within the Component (including third-party service providers) are trustworthy and meet established security criteria for those positions.

(2) Ensure Non-United States (U.S.) citizens are not authorized to access or assist in the development, operation, management or maintenance of Component IT systems, unless a waiver has been granted by the Component Head, with the concurrence of the Department Chief Information Officer (CIO) and Department Security Officer (DSO).

(3) Ensure Component information and IT systems are protected during and after personnel actions such as terminations and transfers.

(4) Employ formal sanctions for personnel failing to comply with Department security policy and procedures.

b. **Physical and Environmental Protection.** In accordance with DOJ IT Security Standard – Physical and Environmental Protection (PE) Control Family, Components shall:

(1) Limit physical access to IT systems, equipment and the respective operating environments to authorized individuals and monitor and log all such accesses.

(2) Protect the physical plant and support infrastructure for IT systems.

(3) Provide supporting utilities for IT systems.

(4) Protect IT systems against environmental hazards.

(5) Provide appropriate environmental controls in facilities containing information systems.

c. **Contingency Planning.** In accordance with DOJ IT Security Standard – Contingency Planning (CP) Control Family, Components shall establish, maintain and effectively implement plans for emergency response, backup operations and post-disaster recovery for Component IT systems to ensure the availability of critical IT resources and continuity of operations in emergency situations.

d. **Configuration Management.** In accordance with DOJ IT Security Standard – Configuration Management (CM) Control Family, Components shall:

(1) Establish and maintain baseline configurations and inventories of Component IT systems (including hardware, software, firmware and documentation) throughout the respective system development life cycle.

(2) Establish a configuration change control process to ensure proposed changes are evaluated, tested, properly approved and documented before being put into production.

(3) Establish and enforce security settings consistent with the information system operational requirements and Department commonly accepted security configurations (e.g., Federal Desktop Core Configuration) and validate those controls through Department approved tools.

e. **Maintenance.** In accordance with DOJ IT Security Standard – Maintenance (MA) Control Family, Components shall:

(1) Perform periodic and timely maintenance on Component IT systems.

(2) Provide effective controls on the tools, techniques, mechanisms and personnel used to conduct on-site and remote IT system maintenance.

f. **System and Information Integrity.** In accordance with DOJ IT Security Standard – System and Information Integrity (SI) Control Family, Components shall:

(1) Identify, report and correct information and information system flaws in a timely manner.

(2) Provide protection from malicious code at appropriate locations within Component IT systems.

(3) Monitor IT system security alerts and advisories and take appropriate actions in response.

g. **Media Protection.** In accordance with DOJ IT Security Standard – Media Protection (MP) Control Family, Components shall:

(1) Protect IT system media, both paper and digital.

(2) Encrypt sensitive and classified information transported outside of the agency's secured, physical perimeter in digital format (including information transported on removable media such as USB drives, CDs, DVDs and on portable/mobile devices such as laptop computers and/or personal digital assistants) using FIPS 140-2 validated or NSA approved encryption, as appropriate.

(3) Limit access to information on IT system media to authorized users.

(4) Sanitize or destroy IT system media before disposal or release for reuse.

(5) Stipulate in contracts for equipment maintenance warranty that equipment to be removed from the Component's physically protected offices shall be sanitized before removal.

h. **Incident Response.** In accordance with DOJ IT Security Standard – Incident Response (IR) Control Family, Components shall:

(1) Establish an operational incident handling capability for Component IT systems that includes adequate preparation, detection, analysis, containment, recovery and user response activities in coordination with the Department of Justice Computer Emergency Response Team (DOJCERT).

(2) Track, document and report incidents to appropriate Department officials and/or authorities.

(3) Provide Department forensics and law enforcement personnel access to media and devices required for investigation, when appropriate.

(4) Assist with digital forensics on electronic devices and/or associated media.

(5) Maintain a chain of custody to record the handling and transfer of media and devices to support investigations and forensics.

i. **Awareness and Training.** In accordance with DOJ IT Security Standard – Awareness and Training (AT) Control Family, Components shall:

(1) Ensure managers and users of Component and Department IT systems are aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policy, standards, instructions, regulations, or procedures related to the security of Component and Department IT systems and data, including digital and paper.

(2) Ensure Component personnel are adequately trained to carry out their assigned IT security-related duties and responsibilities.

5. Technical Security Policy

a. **Identification and Authentication.** In accordance with DOJ IT Security Standard – Identification and Authentication (IA) Control Family, Component IT systems shall:

(1) Identify IT system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to Component IT systems.

(2) Allow remote access only with two-factor authentication where one factor is provided by a device separate from the computer gaining access. (See Chapter 2, paragraph 13)

b. **Access Control.** In accordance with DOJ IT Security Standard – Access Control (AC) Control Family, Component IT systems shall:

(1) Limit IT system access to authorized users, processes acting on behalf of authorized users, or devices (including other IT systems) and to the types of transactions and functions authorized users are permitted to exercise.

(2) Restrict remote access to Government or contractor owned systems. Remote access from personally owned and “public computers” is prohibited. (See Chapter 2, paragraph 13)

(3) Prohibit automatic forwarding of email received in a Component or Department email system to or through a non-Department email system, unless the Authorizing Official grants a waiver.

c. **Audit and Accountability.** In accordance with DOJ IT Security Standard – Audit and Accountability (AU) Control Family, Component IT systems shall:

(1) Create, protect and retain IT system audit records to the extent needed to enable security monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate IT system activity.

(2) Ensure the actions of individual IT system users can be uniquely traced to those users so they can be held accountable for their actions.

(3) Provide direct, real-time or near real-time electronic data feeds of all relevant security monitoring and auditing data (e.g., Firewall event logs, Intrusion Detection or Prevention system alerts and logs, network and desktop antivirus event logs, content scanning and filtering system logs, DHCP, DNS, etc.) to the Department Security Operations Center (SOC) systems unless the Department CIO grants a waiver based upon assessed risk, mitigating controls and operation requirements.

d. **System and Communications Protection.** In accordance with DOJ IT Security Standard – System and Communications Protection (SC) Control Family:

(1) All connections to external networks supporting external access and/or remote access to Department or Component IT systems shall be obtained through a Trusted Internet Connection Access Provider (TICAP), unless the Department CIO grants a waiver based upon assessed risk, mitigation controls and operational requirements.

(2) The Department shall maintain and publish a list of known malicious resources and sites. Components shall implement blocking of these resources and sites at boundary protection devices. Exceptions to allow access to resources and/or sites on this list must be approved by the Component CIO and reported to the Department's Security Operations Center.

(3) Components shall monitor, control and protect Component communications (e.g., information transmitted or received by Component IT systems) at the external boundaries and key internal boundaries of the IT systems.

(4) Component systems shall utilize approved cryptographic mechanisms or protected distribution systems to protect the confidentiality and integrity of information transmitted beyond the secured physical perimeter.

(5) Remote access computers shall use an encrypted VPN to connect to Component information systems.

(6) Components shall employ architectural designs, software development techniques and systems engineering principles that promote effective IT security within Component IT systems.

(7) Components shall be prohibited from deploying systems, technologies, or services (e.g., encapsulation, tunneling, encryption) inconsistent with department security enterprise architecture requirements (e.g., Firewalls, Intrusion Detection Systems, Antivirus systems, content scanning and filtering systems), unless the Department CIO grants a waiver based upon assessed risk, mitigating controls, and operational requirements, prior to operational use.

6. National Security Systems and Sensitive Compartmented Information (SCI) IT Systems

Security policy for systems processing collateral (i.e., non-SCI) national security information is established by the Committee on National Security Systems (CNSS). Security policy for systems processing Sensitive Compartmented Information (SCI) is established by Director of National Intelligence (DNI) in Intelligence Community Directive (ICD) 503, Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation. The Department Security Officer (DSO) is responsible for obtaining accreditation of IT systems processing SCI.

Components shall conform to DOJ Security Program Operating Manual (SPOM), ICD 503 and CNSS policies to manage the security of their National Security Systems. Components shall use NIST SP 800-59, "Guideline for Identifying an Information System as a National Security System," to identify National Security Systems.

7. Classified Laptop and Mobile Computing Devices

The Department Security Officer (DSO) and Department Chief Information Officer (CIO) shall approve, in writing, the processing of classified information on laptops and mobile computing devices. Requests for approval shall be submitted through the Chief Information Security Officer who will obtain the approvals. DOJ IT Security Standard – Classified Laptop and Standalone Computers Security Policy outlines the requirements for laptop computers that process or store classified information, including requirements for standalone computers that process or store classified information.

8. Use of DOJ IT Resources Outside US Territory.

The Department Security Officer (DSO) and Department Chief Information Officer (CIO) shall approve, in writing, the transportation or use of DOJ computers outside of US Territory. Components may approve the use of Department telephones, including BlackBerry smartphones and similar devices, outside US Territory. Components shall:

a. Limit data taken outside US Territory to that which is needed to accomplish the purpose of the travel.

b. Prevent remote access to DOJ IT systems from outside US Territory, with the exception of systems specifically accredited for such access and email via smartphones or personal digital assistants (PDAs).

c. Inspect computers, smartphones, PDAs and media that have been transported outside US Territory for compromise prior to any physical connection to a Component or Department system. If the Component can not conduct such an inspection, it shall reimage the computer or sanitize the media.

9. Facsimile

a. All classified and sensitive facsimile transmissions shall be preceded by a cover sheet containing the following information:

(1) The classification or sensitivity of the information.

(2) The name, office and voice/fax telephone numbers for the recipient(s) and sender.

(3) A warning banner with instructions to the recipient if the facsimile was received in error.

b. Classified information shall be encrypted for transmission with National Security Agency (NSA)-approved encryption.

CHAPTER 2. ISSUE-SPECIFIC SECURITY POLICIES

Whereas program policy is intended to address the broad organization wide computer security program, the issue-specific policies in this chapter focus on areas of current relevance and concern to the Department.

10. Sensitive and Personally Identifiable Information (PII)

The term “personally identifiable information” refers to information that can be used to distinguish or trace individuals’ identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. Loss or disclosure of sensitive information not only has a serious negative impact on our law enforcement and other critical functions, but also diminishes the public trust in our operations. There is inherent risk in carrying such data on mobile computers and devices. The purpose of this policy is to compensate for the lack of

physical security controls when information is removed from or accessed from outside the agency location. Components shall:

a. Reduce the volume of collected and retained PII to the minimum necessary.

b. Limit access to only those individuals who must have such access.

c. Categorize sensitive PII and information systems processing such information as moderate or high impact.

d. Not remove sensitive PII from Component controlled IT systems or facilities unless required (e.g., court filings, debt collection activities).

e. Log all computer-readable data extracts from databases holding sensitive information and ensure each extract including sensitive data has been erased within 90 days or its use is still required. All DOJ information is considered sensitive information unless designated as non-sensitive by the Component head.

f. Notify the DOJ Computer Emergency Readiness Team (DOJCERT) of all incidents involving known loss of sensitive data and PII as an Unauthorized Access incident (Category 1) within one hour of discovery. Loss of any data storage devices, such as laptops, flash drives, disks and tapes, should be reported as an Incident under Investigation (Category 6) within the same one hour time frame. DOJCERT will notify the US-CERT and the Department CIO.

g. Ensure all contracts involving the processing and storage of PII comply with Department policies on remote access and security incident reporting.

11. External Information Systems

External information systems are information systems or components of information systems that are outside of the accreditation boundary established by the Component and for which the Component typically has no direct control over the application of required security controls or the assessment of security control effectiveness. External access includes interconnections between Department IT systems and non-Department IT systems, and between Component IT systems internal to the Department, where there is direct connection of two or more IT systems for the purpose of sharing data and other information resources. External access also includes connections to the Internet.

External access presents both security concerns and resource management issues. The goal of this policy is to ensure Components can effectively, efficiently and safely exchange data with other government and private sector systems, and can utilize resources available on the Internet to accomplish their missions.

Components shall:

a. Obtain all connections to external networks that support external access and/or remote access through a Trusted Internet Connection Access Provider (TICAP), unless the Department CIO grants a waiver based upon assessed risk, mitigation controls and operational requirements.

b. Be prohibited from deploying systems, technologies, or services (e.g., encapsulation, tunneling, encryption, etc) inconsistent with department security architecture requirements (e.g., Firewalls, Intrusion Detection or Prevention Systems, Antivirus systems, content scanning and filtering systems, etc.), unless the Department CIO grants a waiver based upon assessed risk, mitigating controls, and operational requirements, prior to operational use.

12. Protection of Mobile Computers/Devices and Removable Media

Information physically transported outside of the Department's secured physical perimeter is more vulnerable to compromise. The intent of this policy is to compensate for the protections no longer offered by the physical security controls when information is removed from the Component location.

Information on mobile computers/devices (e.g., notebook computers, personal digital assistants) and removable media shall be encrypted using FIPS 140-2 validated or NSA approved encryption mechanism, based on the classification of information processed on the device; unless the data is determined to be non-sensitive, in writing, by the Component Head or principal deputy. Mobile computers shall utilize anti-viral software and a host-based firewall mechanism. Components shall ensure all security related updates are installed on mobile computers/devices. Information should be deleted from mobile computers/devices when no longer needed.

13. Remote Access to DOJ Systems

Remote access is any access to a Component's nonpublic information system by a user (or an information system) communicating through an external, non-Department-controlled network (e.g., the Internet) using a Component controlled computer. Remote access presents additional security concerns since the Component has no direct control over the application of required security controls or the assessment of security control effectiveness of the connecting network. The goal of this policy is to ensure Components can safely utilize remote access to better accomplish their missions.

a. Remote access systems shall be restricted to Government owned or contractor owned systems. Remote access from personally owned or "public computers" is prohibited.

   (1) Remote computers shall employ anti-viral software, firewalls and encryption of stored data using FIPS 140-2 validated or NSA approved encryption.

(2) Remote computers shall have all current and applicable Operating System (OS) and application security updates in place.

(3) Components shall utilize a configuration management system for remote access computers to ensure the remote access computer has the Component approved security software in place, the OS is fully patched, antivirus software is installed and up-to-date and a personal firewall is enabled.

(4) Remote access computers shall use two-factor authentication where one factor is provided by a device separate from the computer gaining access.

(5) Remote access computers shall use an encrypted VPN to connect to Department information systems.

(6) Remote access computers shall not be connected to any other network when connected to a Department IT system.

(7) Remote access login sessions shall be restricted to a single operating system and a single network interface card when connected to a Department IT system.

14. Contractors

The Components and Department may utilize contractors to develop, operate and/or maintain IT systems on their behalf. Contractors may be granted access to Component and Department IT systems and information in order to perform work specified under the contract. Access may be from Component or Department owned computers or from contractor owned computers. Contractors may process Component and Department information on contractor owned equipment, either within or outside DOJ space. In all these situations, the contractors and their sub-contractors, their personnel and their IT systems and devices shall fall under the provisions of this order, and the contract shall identity IT security requirements.

All connections to external networks supporting access to DOJ hosted resources (e.g., Government owned web sites, applications, email systems) shall be obtained through a Trusted Internet Connection Access Provider (TICAP), unless the Department CIO grants a waiver based upon assessed risk, mitigation controls and operational requirements.

When the contract requires or allows contractor IT systems to be used, whether to access Component or Department IT systems and/or information or to process or store Component or Department information, the contract shall require the contractor IT systems be certified, accredited and operated pursuant to a valid Authority to Operate (ATO). The ATO shall be issued by a Component Authorizing Official based on this policy. If the contractor utilizes its own internal C&A process it must submit the C&A package to the Component Authorizing Official. If the Component Authorizing Official determines the C&A process

meets the Department standards, he or she may issue an ATO based on the package. Contractors using individual devices under the contract shall provide the Contracting Officer's Technical Representative (COTR) an inventory of such devices and shall operate such devices pursuant to this policy, including all incident response requirements. Contractors and contractor systems shall be subject to the same FISMA data calls as other DOJ systems.

Upon termination of contract work, all DOJ information shall be removed from contractor owned IT equipment. Certification of data removal shall be performed by the contract's project manager and a letter confirming certification shall be delivered to the Contracting Officer within 15 days of the termination of the contract.

CHAPTER 3. DETERMINING SECURITY CONTROL REQUIREMENTS

15. Applicability

The standard security control requirements in this Chapter are applicable to all DOJ IT systems. DOJ IT systems that process National Security Information (NSI) must meet any additional requirements specified by the Committee on National Security Systems (CNSS). DOJ IT systems that process Sensitive Compartmented Information (SCI) must meet any additional requirements specified by the Director of National Intelligence (DNI). If there is a conflict in requirements for systems processing NSI or SCI, the CNSS or DNI requirements shall govern. Components shall use NIST SP 800-59, "Guideline for Identifying an Information System as a National Security System," to identify National Security Systems.

16. Categorize information types and information systems

a. Components shall categorize all Department IT systems as low-impact, moderate-impact, or high-impact, in accordance with Federal Information Processing Standards (FIPS) 199 and 200, or applicable standards for national security systems, as partially implemented in the Department-approved Cyber Security Assessment and Management (CSAM) Toolkit. This process establishes security categories for information types and information systems. The security categories are based on the potential impact on a Component should certain events occur that jeopardize the information and information systems needed by the Component to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions and protect individuals. The impact value for a system shall be the highest value (i.e., high water mark) from those determined for each type of information resident on the system.

b. The Component's risk assessment (threat and vulnerability information) and mission criticality indicators are given manual consideration regarding any required adjustments in the categorization results. Rationale for deviations from the recommended security categorizations must be documented in the System Security Plan. Designated senior-level

officials within the Component shall review and approve the security categorizations. Documented results of this approval are captured in the System Security Plan.

17. Select, tailor and supplement initial baseline security controls

a. The Department has developed IT Security Standards based on the security control families outlined in Federal and National standards, supplemented with additional Department standards. The Department's IT Security Standards outline, in specific detail, the requirements for achieving the high-level goals within this Order. The DOJ IT Security Standards represent minimum DOJ IT security control requirements, supplement this Order and are required for use in accordance with the terms and conditions expressed in the Standards. The requirements in the Standards are implemented in CSAM.

b. Subsequent to the security categorization process, Components shall select an appropriate set of security controls and assurance requirements for their information systems that satisfy the minimum security requirements set forth in these standards and are tailored (enhanced or limited) based on the results of a risk assessment and local conditions, including Component- or system-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.

c. The information system authorizing official shall determine if the control set in the information system security plan is appropriate for securing the information system to an acceptable level of operational risk to the Component. Components shall document the authorizing official's approval of the initial set of tailored security controls in the System Security Plan, including the Component's rationales for any refinements or adjustments to the baseline set of controls.

18. Implement security controls

Components shall then implement the security controls in the information system in accordance with the System Security Plan. Authorizing officials are better positioned to make mission risk determinations based on the known vulnerabilities remaining in the information system after the implementation of an agreed-upon set of security controls.

19. Assess and Authorize the implemented controls

Components shall assess the security controls using appropriate methods and procedures (e.g., CSAM) to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system. The system authorizing official shall authorize the information system operation based upon a determination of the risk to Departmental operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.

20. Monitor

a. Components shall monitor the information system on a continuous basis for changes to the information system or its operational environment, the information system security plan boundaries, or other conditions (e.g., threat and risk factors), conducting security impact analyses of the associated changes, updating the information System Security Plan (and other relevant information system documentation as appropriate) and report changes to the security status of the system to appropriate officials on a regular basis.

b. Significant changes to the system require reaccreditation by the information system's Authorizing Official. Examples of changes to an information system that should be reviewed for possible reaccreditation include:

(1) installation of a new or upgraded operating system, middleware component, or application;

(2) modifications to system ports, protocols, or services;

(3) installation of a new or upgraded hardware platform or firmware component; or

(4) modifications to cryptographic modules or services;

(5) additional connections to information systems outside the accreditation boundary;

(6) functional changes or enhancements to the system that affect its mission criticality, information types, user base, or classification of data supported by the information system.

c. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reaccreditation action.

d. Reauthorization should be avoided in situations where the continuous monitoring process provides the necessary and sufficient information to authorizing officials to manage the potential risk arising from the information system changes.

CHAPTER 4. ROLES AND RESPONSIBILITIES

21. Department Chief Information Officer

Per the Clinger Cohen Act of 1996, the Chief Information Officer (CIO), who also serves as Deputy Assistant Attorney General, Information Resources Management (DAAG/IRM), advises and assists the Attorney General, the Deputy Attorney General, the Assistant Attorney General for Administration and other senior staff in order to ensure the Department

plans, acquires, manages and uses Information Technology (IT) in a manner that enhances mission accomplishment; improves work processes and reduces paperwork; provides sufficient protection for the privacy of personal information; promotes citizen-centered electronic government; and is consistent with all applicable Federal laws and directives. The Department CIO, in addition to the responsibilities outlined in Department Order 2880.1B, Information Resources Management Program, shall be responsible for:

a. Ensuring the Department's IT security program is established and implemented in compliance with Federal laws and regulations.

b. Issuing IT security policy, standards and guidelines to address IT security planning, management and implementation.

c. Developing and/or managing enterprise IT control techniques and technologies while considering Department Component infrastructure and resources and developing and/or managing enterprise security management tools.

d. Reviewing and evaluating the implementation of Department Component program and system security controls in accordance with Department's IT security policy, standards and guidelines.

e. Developing and maintaining the Department's IT Security Program Management Plan (PMP) in accordance with Federal laws and regulations.

f. Developing, implementing and managing a Department-wide Plan of Action and Milestone (POAM) process to correct IT security weaknesses.

g. Requiring Components and program officials to implement Department policy, standards and guidance in the absence of an approved waiver (where applicable), or justification for the use of compensating controls, including a formal assessment and acceptance of risk.

h. Ensuring senior agency officials provide IT security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of:

   (1) Information collected or maintained by or on behalf of the Department.

   (2) IT systems used or operated by an agency, or by a contractor of an agency, or other organization on behalf of an agency.

i. Enforcing Department IT security policy, including levying sanctions on Components for non-compliance.

j. Developing and maintaining a central repository of information on new and emerging technologies. Coordinating and approving any evaluations of new and emerging technologies by Components.

k. Coordinating with the Department Security Officer (DSO) on Sensitive Compartmented Information (SCI) IT systems.

l. Ensuring all Department personnel with access to Department networks and all individuals at contractor facilities working on Department systems, information, or providing services, receive annual IT security awareness training.

m. Ensuring IT security management processes are integrated with the Department and/or Component strategic and operational planning processes.

n. Concurring with or disapproving waiver requests relating to non-United States (U.S.) citizens accessing or assisting in the development, operation, management, or maintenance of Department IT systems.

o. Approving and monitoring waivers to IT security requirements (other than waivers relating to non-U.S. citizens accessing or assisting the development, operation, management, or maintenance of Department IT systems).

p. Approving encryption technologies that are not FIPS 140-2 validated in those situations where FIPS-validated products are not available.

q. Appointing a Chief Information Security Officer (CISO) to carry out the Department-wide IT security program as required by the Federal Information Security Management Act (FISMA).

r. Establishing an IT Security Governance Committee (ITSGC) to be chaired by the Department CIO and consisting of the Deputy Department CIOs and selected Component CIOs. The ITSGC shall be the focal point for providing strategic direction on Department level initiatives.

s. Establishing an IT Security Council (ITSC) with supporting project teams composed of lead-Component IT security personnel.

t. Reporting to the Attorney General and Office of Management and Budget (OMB) on the status of the Department's IT Security Program.

22. Chief Information Security Officer

The Chief Information Security Officer (CISO) chairs the Department's ITSC and serves as the principal security leader for the Department to implement the requirements of FISMA. The CISO also serves as the Department CIO's liaison to Federal agencies for all matters

relating implementation of IT security and the Department's IT Security Program. The Department CISO shall be responsible for:

a. Developing standards and guidelines for conducting risk assessments to assess risk and determine needs.

b. Implementing Department-wide policy and procedures for related controls to cost-effectively reduce risks to an acceptable level.

c. Monitoring, evaluating and periodically testing IT security controls and techniques to ensure they are effectively implemented.

d. Developing and maintaining a Department-wide IT security program.

e. Providing leadership for the ITSC to execute Department-wide management and implementation of the Department's IT security program.

f. Identifying and developing common security controls and managing the implementation and assessment of common security controls.

g. Ensuring and promoting a comprehensive IT security training program for both privileged and general users.

h. Assessing waiver requests for Department's IT Security Standards on behalf of the Department Chief Information Officer (CIO).

i. Preparing the annual and quarterly Federal Information Security Management Act (FISMA) reports for the Department CIO.

j. Ensuring compliance with monthly reporting on the effectiveness of Component IT security programs, including progress of remedial actions.

k. Identifying IT security management and reporting tools through the IT Security Council (ITSC) for use throughout the Department.

l. Assisting senior Department Component IT security officials in their responsibilities through the ITSC.

23. Department Security Officer

The Department Security Officer (DSO) conducts security compliance reviews to assess the overall effectiveness of security program implementation across the Department, including IT security. The DSO ensures all IT security reviews that require system testing are coordinated with the Department CIO and all IT security-related findings are reported to the Department CIO. The DSO shall be responsible for:

a. Providing advice to the Department CIO on security program areas affecting IT.

b. Providing advice and recommendations to the Department CIO on waiver requests.

c. Concurring with or disapproving requests for waivers relating to non-United States (U.S.) citizens accessing or assisting in the development, operation, management, or maintenance of Department IT systems.

d. Ensuring the development and implementation of Department-wide policy and procedures to govern: TEMPEST; Technical Surveillance Countermeasures (TSCM); Personnel Security; Physical and Environmental Security; Storage and Marking; Media Disposal; Media Reuse; Communications Security (COMSEC) materials; facsimile security; copier security; and those aspects of the DSO's responsibilities for Personnel Security; Document Security; Physical Security; COMSEC; and Emergency Planning described in Department Order 2600.2C.

24. Component Heads or Their Designee(s)

The Component Head or his/her designee(s) shall establish and maintain a Component-wide IT security program to secure the Component's IT systems, networks and data in accordance with Department policy, procedures and guidance. The Component Head or designee(s) work with the Department Chief Information Security Officer (CISO) through the IT Security Governance Committee and IT Security Council to carry out the following responsibilities at the Component level:

a. Implementing Department policy, standards and guidelines.

b. Implementing the Department's IT Security Program Management Plan at Component and system level, and reporting results in accordance with Office of the CIO (OCIO) guidelines.

c. Ensuring the completion of monitoring, testing and evaluation of the effectiveness of IT security policy, procedures, practices and security controls to be performed with a frequency depending on risk, as directed by ITSS.

d. Ensuring the completion of periodic assessments of risk, including the magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information and IT systems that support the operations and assets of the Department.

e. Developing, implementing, managing and prioritizing corrective plans of actions and milestones to correct known weaknesses in IT security using the department-wide POAM process.

f. Reporting quarterly in accordance with guidance issued by Justice Management Division (JMD) or the Department CIO, on the status of their IT security programs to the Department CIO and CISO.

g. Integrating security in the Capital Planning Investment Control (CPIC) process.

h. Assigning roles and responsibilities within the Component (e.g., Component ITSC member, Component CIO, Authorizing Official, Certification Agent, Information System Owner, Information Owner, User Representative, Information System Security Officer).

i. Coordinating with the OCIO any evaluations of new technologies that could impact Department or enterprise services.

j. Participating with other Components and the OCIO in evaluating and selecting IT security tools for use within the Department and obtaining Department CIO approval for non-enterprise IT security solutions.

k. Establishing procedures to ensure software installed on Component IT systems is in compliance with applicable copyright laws and is incorporated into the IT system's life cycle management process.

l. Approving, with the concurrence of the Department CIO and Department Security Officer (DSO), waivers relating to non-United States (U.S.) citizens accessing or assisting in the development, operation, management, or maintenance of Department IT systems, and monitoring those waivers.

m. Ensuring all Component personnel with access to Department networks and all individuals at contractor facilities working on Department systems, information, or providing services, receive annual IT security awareness training.

CHAPTER 5. AGENCY-WIDE PROGRAM IMPLEMENTATION

25. Core Program

a. The Department shall develop and manage an agency-wide IT Security Program, executed through the Department's IT Security Program Management Plan (PMP), consistent with the laws and regulations affecting IT security. The Department's IT security management approach shall employ a collaborative and coordinated effort to maximize available resources and protect Department IT systems and operations.

b. The Department Chief Information Officer (CIO) shall establish security governance through the use of appropriate committees to provide a systematic forum to assist in the accomplishment of established Department IT security objectives.

26. IT Security Management Strategy

The IT security management strategy used by the Department shall be based on the risk management concepts found in Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems," the Federal Information Security Management Act (FISMA), and other Federal guidance. The risk management principles in the proceeding sections provide the framework for the Department's IT security management strategy. An important factor in effectively implementing these principles is linking them in a cycle that ensures IT security policy addresses current risks on an ongoing basis.

a. Central Focal Point

The Information Technology Security Staff (ITSS) shall serve as the central focal point for IT security in the Department. The ITSS shall provide Department-wide management and implementation of the Department IT security program. The ITSS and the Components shall provide a collaborative team to manage the accomplishment of priorities for achieving business objectives and complying with FISMA; Homeland Security Presidential Directives; Presidential Decision Directives/ Presidential Directives; Executive Orders; Office of Management and Budget (OMB); National Institute of Standards and Technology (NIST); Committee on National Security Systems (CNSS); Director of National Intelligence (DNI) Directives; and Department IT security requirements.

b. Follow a Department-wide common Security Strategy

The Department shall follow a common Security Strategy that defines the common security goals for all Components. These goals shall outline the Department's security posture both internally and externally while taking into account the respective business needs and missions of each Component. The Department's common Security Strategy will be strengthened by the adoption of a common IT Security Architecture developed to ensure information systems remain secure throughout their entire lifecycle. The security needs and requirements shall be identified early on in the process and be funded appropriately.

c. New and emerging technologies

Information technology is a dynamic field with new and emerging technologies constantly being identified that could assist the Department to better accomplish its constantly evolving mission. The OCIO shall provide a central repository of information on these technologies. Components shall coordinate with this office prior to undertaking any evaluation of new or emerging technologies. This office shall maintain all evaluations and make them available to Components to leverage work already performed and to avoid duplication of effort.

d. Implement Policy and Procedures

(1) The Department's IT Security policy shall clearly address the Department's IT security needs and serve as the foundation for the Department's IT security program. Policy shall represent the primary mechanism for senior management to communicate its IT security requirements to the Components. Policy shall be adjusted (as required) and shall be related to the risk of the Department or Components not being able to perform their functions.

(2) The Department's IT Security Standards shall provide detailed procedures for implementing Department policy and shall be practical to implement. The IT Security Standards shall outline specific requirements for accomplishing the Department's security goals. The Department's IT Security Standards are divided into the following three general security control classes: (i) Management; (ii) Operational; and (iii) Technical.

e. Promote Awareness

All users of Department IT systems shall be continually educated on risks and related policy as they are more likely to support and comply with the policy if they understand the purpose behind the policy and their associated responsibilities.

f. Manage Risk and Determine Needs

(1) Senior management views IT security as an "enabler." Based on a thorough examination of the risks, Department and Component Senior management shall assume risks and take responsibility for the operation of systems based on risks identified in assessments balanced by the impact the IT system has on Department operations. Additionally, the risk management process shall be continually evaluated to ensure it addresses the current threats to Department IT systems.

(2) The Department's risk management methodology shall present a formal, structured approach for developing risk assessments for IT systems that are part of a major application or general support system. This methodology shall provide a uniform standard for evaluating IT security risks to IT systems operating within the Department. The primary focus of this methodology shall be on the IT system's mission, not IT assets. Since risk management is an essential management function, Department IT system owners and IT security managers shall use this methodology when assessing risks and prioritizing resources for certifying and accrediting Department IT systems.

g. Monitor and Evaluate

The Department's IT security program shall include continually monitoring and assessing IT security policy and IT security controls to ensure they remain appropriate and effective. Monitoring control effectiveness and compliance with policy shall be

incorporated within the cycle of managing the Department's IT security program, and shall be performed through the use of automated software tools when possible.

APPENDIX 1. REFERENCES

The following references are applicable to the Department IT security policy. Unless otherwise stated, all references to publications (e.g., NIST Federal Information Processing Standards, NIST Special Publications) are to the most recent version of the referenced publication.

1. Congressional Mandates

a. Clinger Cohen Act of 1996, (Pub. L. 104-106, 110 Stat. 186); and (Pub. L. 104-208, 110 Stat. 3009).
b. Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030.
c. Computer Security Act of 1987, 15 U.S.C. § 272, 278h, 278g-3, 278g-4.
d. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511.
e. E-Government Act of 2002, PL 107-347, 44 U.S.C. Ch 35.
f. Federal Information Security Management Act of 2002 (FISMA), Pub. L. 107-347, 116 Stat. 2899.
g. Federal Managers Financial Integrity Act of 1982 (FMFIA), Pub. L. 97-255, 96 Stat. 814.
h. Freedom of Information Act (FOIA), 5 U.S.C. § 552.
i. Paperwork Reduction Act of 1995 (PRA), Pub. L. 104-13, 109 Stat. 163; 44 U.S.C. 3501-3520.
j. Privacy Act of 1974, 5 U.S.C. § 552a.

2. Federal/Departmental Regulations/Guidance

a. 28 C.F.R. 45.4, Personal Use of Government Property.
b. 36 C.F.R. 1194, Electronic and Information Technology Accessibility Standards (65 FR 80500).
c. 41 C.F.R. 101-35, Telecommunications Management Policy.
d. Committee on National Security Systems Instruction (CNSSI) No. 7000, TEMPEST Countermeasures for Facilities.
e. CNSS Policy (CNSSP) No. 6, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems
f. CNSSI No. 4009 National Information Assurance Glossary.
g. CNSSI No. 4016, National Information Assurance Training Standard For Risk Analysts
h. CNSS NSS Instruction 1199, Security Categorization for National Security Systems and Information (ODNI/CIO Draft).
i. CNSS NSS Instruction 1218 (ODNI/CIO Draft), Guide for Developing Security Plans for National Security Information Systems.
j. CNSS NSS Instruction 1230 (ODNI/CIO Draft), Risk Management Guide for National Security Information Technology Systems, provides guidance on the assessment and mitigation of risk as part of an overall risk management process.
k. CNSS NSS Instruction 1237 (Draft), Guide for the Security Certification and Accreditation of National Security Information Systems, provides guidance on the security authorization of NSSs.

l. CNSS NSS Instruction No. 1253 (ODNI/CIO Draft), Security Control Catalog for National 9 Security Systems.
m. CNSS NSS Instruction 1253A (Draft), Guide for Assessing the Security Controls in National Security Information Systems, provides guidance for determining the effectiveness of security controls.
n. CNSS NSS Instruction 1260 (Draft), Security Categorization of National Security Information and Information Systems.
o. DCID 6/5, Policy for Protection of Certain Non-SCI Sources and Methods Information (SAMI).
p. DCID 6/9, Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs).
q. Department of Justice (DOJ) Order 2600.2C, Security Programs and Responsibilities.
r. DOJ Security Program Operating Manual (SPOM).
s. DOJ Order 2610.2A, Employment Security Regulations. Government Paperwork Elimination Act, 44 USC 3504.
t. DOJ Order 2880.1B, Information Resources Management.
u. DOJ Order 2740.1, Use and Monitoring of DOJ Computers and Computer Systems.
v. Federal Information Processing Standard (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules.
w. FIPS Publication 199, Standards for Security Categorization of Federal Information Systems.
x. FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems.
y. FIPS Publication 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors.
z. Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements.
aa. Intelligence Community Directive Number 503, Intelligence Community Information Technology Systems Security, Risk Management, Certification and Accreditation.
bb. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook.
cc. NIST SP 800-14, Generally Accepted Principles and Practices for Security Information Technology Systems.
dd. NIST SP 800-16, Information Technology Security Training Requirements.
ee. NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems
ff. NIST SP 800-27, Engineering Principles for Information Technology Security.
gg. NIST SP 800-28, Guidelines on Active Content and Mobile Code.
hh. NIST SP 800-30, Risk Management Guide for Information Technology Systems.
ii. NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.
jj. NIST SP 800-35, Guide to Information Technology Security Services.
kk. NIST SP 800-36, Guide to Selecting Information Technology Security Products.
ll. NIST SP 800-37, Guide for the Security Certification and Accreditation for Federal Information Systems.
mm. NIST SP 800-39, Managing Risk from Information Systems.

nn. NIST SP 800-40, Creating a Patch and Vulnerability Management Program.
oo. NIST SP 800-41, Guidelines on Firewalls and Firewall Policy.
pp. NIST SP 800-44, Guidelines on Securing Public Web Servers.
qq. NIST SP 800-45, Guidelines on Electronic Mail Security
rr. NIST SP 800-46, Security for Telecommuting and Broadband Communications.
ss. NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems.
tt. NIST SP 800-48, Guide to Securing Legacy IEEE 802.11 Wireless Networks.
uu. NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.
vv. NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations.
ww. NIST SP 800-53, Recommended Security Controls for Information Systems.
xx. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.
yy. NIST SP 800-54, Border Gateway Protocol Security.
zz. NIST SP 800-55, Security Metrics Guide for Information Technology Systems.
aaa. NIST SP 800-59, Guideline for Identifying an Information System as a National Security System.
bbb. NIST SP 800-60 (Vol. I and II), Guide for Mapping Type of Information and Information Systems to Security Categories.
ccc. NIST SP 800-61, Computer Security Incident Handling Guide
ddd. NIST SP 800-63, Electronic Authentication Guideline.
eee. NIST SP 800-64, Security Considerations in the Information System Development Life Cycle.
fff. NIST SP 800-68, Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist.
ggg. NIST SP 800-70, Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers.
hhh. NIST SP 800-76, Biometric Data Specification for Personal Identity Verification.
iii. NIST SP 800-77, Guide to IPsec VPNs.
jjj. NIST SP 800-81, Secure Domain Name System (DNS) Deployment Guide.
kkk. NIST SP 800-83, Guide to Malware Incident Prevention and Handling.
lll. NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.
mmm. NIST SP 800-88, Guidelines for Media Sanitization.
nnn. NIST SP 800-92, Guide to Computer Security Log Management.
ooo. NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS).
ppp. NIST SP 800-95, Guide to Secure Web Services.
qqq. NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.
rrr. NIST SP 800-100, Information Security Handbook: A Guide for Mangers.
sss. NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices.
ttt. NIST SP 800-113, Guide to SSL VPNs.
uuu. NIST SP 800-114, User's Guide to Security External Devices for Telework and Remote Access.

vvv. NIST SP 800-115, Technical Guide to Information Security Testing and Assessment.
www. NIST SP 800-121, Guide to Bluetooth Security.
xxx. NIST SP 800-123, Guide to General Server Security.
yyy. NIST SP 800-124, Guidelines on Cell Phone and PDA Security.
zzz. National Security Agency (NSA)/ Central Security Service (CSS) Policy 9-12, NSA/CSS Storage Device Declassification.
aaaa. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 1000, National Information Assurance C&A Process (NIACAP).
bbbb. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products.
cccc. National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/2-95, RED/BLACK Installation Guidance.

3. Presidential and Office of Management and Budget Guidance

a. Executive Order 12958, Classified National Security Information, as amended.
b. EO 12968, Access to Classified Information.
c. EO 13231, Critical Infrastructure Protection in the Information Age.
d. EO 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans.
e. General Accounting Office (GAO) Federal Information System Control Audit Manual (FISCAM).
f. International Standard 15408, Common Criteria for Information Technology Security Evaluation.
g. Homeland Security Presidential Directive (HSPD) 7, Critical Infrastructure Identification, Prioritization, and Protection,
h. HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors.
i. Memorandum for The Heads of Executive Departments and Agencies, Designation and Sharing of Controlled Unclassified Information (CUI).
j. National Security Directive 42, National Policy for the Security of National Security and Telecommunications and Information Systems.
k. National Security Presidential Directive (NSPD 51) / Homeland Security Presidential Directive (HSPD-20), National Continuity Policy.
l. Office of Management and Budget (OMB) Circular A-127, Financial Management Systems.
m. OMB Circular A-130, Management of Federal Information Resources (with Appendices and periodic revisions).
n. OMB Memorandum 99-18, Privacy Policy on Federal Web Sites.
o. OMB Memorandum 00-13, Privacy Policies and Data Collection on Federal Web Sites.
p. OMB Memorandum 01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy.
q. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies.
r. OMB Memorandum 04-26, Personal Use Policies and “File Sharing” Technology.

s. OMB Memorandum 05-02, Financial Management Systems.
t. OMB Memorandum 06-15, Safeguarding Personally Identifiable Information.
u. OMB Memorandum 06-16, Protection of Sensitive Agency Information.
v. OMB Memorandum 06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments.
w. OMB Memorandum 07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems.
x. OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
y. OMB Memorandum 07-18, Ensuring New Acquisitions Include Common Security Configurations.
z. OMB Memorandum 07-24, Updated Principles for Risk Analysis.
aa. OMB Memorandum 08-05, Implementation of Trusted Internet Connections (TIC).
bb. OMB Memorandum 08-16, Guidance for Trusted Internet Connection Statement of Capability Form (SOC).
cc. OMB Memorandum 08-22, Guidance on the Federal Desktop Core Configuration (FDCC).
dd. OMB Memorandum 08-23, Securing the Federal Government's Domain Name System Infrastructure.
ee. OMB Memorandum 08-27, Guidance for Trusted Internet Connection (TIC) Compliance.
ff. OMB Memorandum 09-02, Information Technology Management Structure and Governance Framework.