# REPORT ON EVALUATION
# OF FLRA FISMA COMPLIANCE
# JULY 2009

2020 Pennsylvania Avenue
Suite 185
Washington, DC 20006

Tel 1-202-386-8510
Fax 1-202-536-4859

www.txdel.com

# CONTENTS

**REPORT ON EVALUATION**
**OF FLRA FISMA COMPLIANCE**

## EXECUTIVE SUMMARY

Txdel, on behalf of the Federal Labor Relations Authority (FLRA), Office of Inspector General, conducted an independent evaluation of the quality and compliance of the FLRA security program with applicable federal computer security laws and regulations. Txdel's evaluation focused on FLRA's information security required by the Federal Information Security Management Act (FISMA).

FLRA has not established adequate security controls in several areas. Specifically, the FLRA information security program does meet responsibilities required for Federal agencies stipulated in FISMA, Section 3544, Federal Agency Responsibilities, National Institutes of Standards and Technology 800-53A - Guide for Assessing the Security Controls in Federal Information Systems, and Office of Budget and Management A-130. The weaknesses identified by this evaluation are attributed to the lack of IT security policies, procedures and process for managing Access Control – w*hich provides a technical means of controlling what information users can utilize, the programs they can run, and the modifications they can implement*; Awareness and Training – *which informs users of the need to protect system resources, developing skills and knowledge*; Audit and Accountability – *which reviews management, operational, and technical controls*; Certification, Accreditation and Security – *which formally tests the security safeguards implemented in the computer system*; Configuration Management – *the process of keeping track of changes to the system and, if needed, approving them*; Contingency Planning – t*he initial actions taken to protect lives and limit damage, the steps that are taken to continue support for critical functions, and the return to normal operations*; Cryptography – e*ncryption of data; can be used to provide many security services, such as electronic signatures and ensuring that data has not been modified*; Identification and Authentication – *the portion of access control that prevents unauthorized people (or unauthorized processes) from entering a computer system*; Incident Response – *the portion of contingency planning that responds to malicious technical threats; Maintenance – the system is almost always modified by the addition of hardware and software and by numerous other events*; Media Protection – *which provides a variety of measures to provide physical and environmental protection and accountability for tapes, diskettes, printouts, and other media*; Physical and Environmental Protection – *which provides measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment*; Planning – *used to help ensure that security is addressed in a comprehensive manner throughout a system's life cycl*e; Personnel Security – *which involves measures taken to safeguard a company's employees and those coming to a place of business*; Risk Assessment – *the process of analyzing and interpreting risk*; System and Services Acquisition – *a detailed list of functional, security, and system requirements*; System and Communications Protection – *which provides protection to information system and communication needed to meet the government and industry standards and requirements*; System and Information Integrity – *which ensures timely, accurate, complete, and consistent information;* and Privacy Protection – *ensuring the protection of Personal Identifiable Information (PII)* - *The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal*

*or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.*

The objective of this evaluation is to assess the FLRA's FISMA compliance in accordance with prevailing Federal security regulations. Our evaluation reviewed aspects of the agency's information technology security functions.

This report was prepared in conjunction with the Inspector General and Txdel. The weaknesses discussed in this report should be viewed as material and should be included in FLRA's Fiscal Year (FY) 2009 report to the Office of Management and Budget (OMB) and congress.

**REPORT ON EVALUATION**
**OF FLRA FISMA COMPLIANCE**

Txdel, on behalf of the Federal Labor Relations Authority (FLRA), Office of Inspector General, conducted an independent evaluation of the quality and compliance of the FLRA security program with applicable federal computer security laws and regulations. Txdel's evaluation focused on FLRA's information security required by the Federal Information Security Management Act (FISMA).

This report was prepared in conjunction with the Inspector General and Txdel. The weaknesses discussed in this report should be viewed as material and should be included in FLRA's Fiscal Year (FY) 2009 report to the Office of Management and Budget (OMB) and congress.

- Introduction
- Background
- Methodology
- Statutory and Related Requirements
- Findings, Recommendations, and Management Comments

## INTRODUCTION

Implementing adequate information security controls is essential to ensuring an organization can effectively meet its mission. The Office of Management and Budget (OMB) and the National Institutes of Standards and Technology (NIST) provides federal agencies guidance for complying with federal laws and regulations. The Office of the Inspector General (OIG) plays an essential role supporting federal agencies by performing annual FISMA evaluations, which assist federal agencies indentifying areas for improvement.

## BACKGROUND

The Federal Labor Relations Authority has not complied with several laws and regulations identified by Office of Management and Budget. The lack of adherence to the aforementioned laws was documented in several of the previous information security evaluations and financial statement audits specifically, 2008 Federal Labor Relations Authority Inspector General FISMA Evaluation, Performance and Accountability Report, FY 2007, and Report on Audit of FLRA Security Programs September 2004. The Inspector General during previous administration did not have a direct and material effect on the Federal Labor Relations Authority Information Technology, Information Technology Security, E-Government and FISMA. However, in 2008, the now former Chief Financial Officer/Acting Chief Information Officer was hired by the Federal Labor Relations Authority during 2008 resigned on September 26, 2008. FLRA senior management recently a new Chief Information Officer (CIO) and the FLRA Chairman is committed to supporting the CIO in improving the information security posture. With that having been said, the new CIO is currently working with contractors to create a certification & accreditation (a

comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, 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); of the general support system (an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people). Which we believe will be a great accomplishment for the FLRA.

## METHODOLOGY

We will conduct the evaluation of FLRA's information system security program in four phases described below along with the primary objectives of each:

**Planning:** Develop the FISMA evaluation work plan program.

**Internal Control Evaluation, Risk Assessment, and Compliance Phase:**

- Review and evaluate the existence and effectiveness of internal controls and compliance with federal laws and regulations.
- Assess FLRA's risks.
- Substantive Testing - Conduct vulnerability tests and network configuration analysis for compliance with FISMA and other federal security requirements.

**Contracted Auditor Phase:**

- Ensure that information technology audit objectives are addressed in accordance with Financial Audit Manual (FAM) and FISMA adequately.
- Substantive Testing - Conduct vulnerability tests and network configuration analysis for compliance with FISMA and other federal security requirements.

**Preparation of Information Technology and FISMA Reporting:**

- Provide oral and written status reports.
- Conduct an exit conference with FLRA's Inspector General.
- Develop draft and final reports.
- Conduct a briefing for FLRA management.
- Solicit management comments.
- Revise the report to include management comments.

We designed our approach to obtain sufficient quantitative and qualitative information on the information system and security program, plans, structures, standards, policies, procedures, and administration to assess and draw conclusions on the adequacy and effectiveness of information system security to safeguard hardware, software, and data. This includes obtaining reasonable assurance that the control structure and framework are suitable and commensurate with perceived risks and magnitude of harm resulting from these risks. Our report deliverable will specifically address control requirements required by OMB to describe

FLRA's level of progress to effectively implement security controls covering the management, operational, and technical control areas.

Evaluation techniques and procedures included interviews with knowledgeable information security management and personnel; observations of information system facilities, hardware, and personnel; review and analysis of FLRA's information system security standards, policies, procedures, and practices; and general and specific control tests.

We discussed our evaluation findings and recommendations with FLRA senior management and will include their responses in this report.

## STATUTORY AND RELATED REQUIREMENTS

Txdel performed an independent evaluation of the quality and compliance of the FLRA security program with applicable federal computer security laws and regulations. Txdel's evaluation will focus on FLRA's information security required by the Federal Information Security Management Act (FISMA).

Txdel's independent evaluation report addresses regulations specified by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) to ensure FLRA management has:

*Periodic assessments of risk*, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization;

*Policies and procedures* that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information system;

*Subordinate plans* for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate;

*Security awareness training* to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks;

*Periodic testing and evaluation* of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;

*A process for planning*, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;

*Procedures for detecting*, reporting, and responding to security incidents;

*Plans and procedures* to ensure continuity of operations for information systems that support the operations and assets of the organization.

In support of this evaluation, the Inspector General (IG) must conduct an independent evaluation of the security program and submit a report that includes findings, observations, conclusions, and recommendations.

To meet these objectives, Txdel evaluated FLRA's implementation of the following criteria, using FISMA and related OMB guidance:

- Federal Information Security Management Act (FISMA) of 2002 (PL 107-347): Provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.
- Government Information Security Reform Act (GISRA) of 2001 (PL 106-398): Requires federal agencies to assess the security of both classified and non-classified systems and to include risk assessment and security needs with each new budget request.
- Computer Fraud and Abuse Act of 1986 (PL 99-474): Established specific protection for fraud and related activities in connection with Federal computers. Such offenses include: intentionally accessing a Federal Interest Computer without authorization and (1) obtaining anything of value (including data), (2) preventing unauthorized use, or (3) altering information.
- Federal Managers Financial Integrity Act of 1982 (PL 97-255): Requires that agency internal control systems be periodically evaluated and the heads of executive agencies report annually on their systems status.
- Paperwork Reduction Act of 1980 (PL 96-511): Defines the process to reduce paperwork and enhance the economy and efficiency of the Government and the private sector by improving Federal information policy-making.
- Federal Records Management Acts of 1976 and 1950 (PL 94-575 and PL 81-754): Requires establishment of standards and procedures to ensure effective records creation, use, maintenance, and disposal.
- Privacy Act of 1974 (PL 93-579): Establishes standards and safeguards for the collection, maintenance, or disclosure of an individual's personal information by federal agencies and grants access to the records that require confidential treatment to that individual.
- Freedom of Information Act of 1974 (PL 90-23): Establishes a set of procedures for the release of governmental records that ensure the principle of openness in government, while guarding against specific harm to governmental and private interests.
- OMB Circular A-123, 1981 & A-123R, 1983: Prescribes policies and standards to be followed by executive agencies in establishing and maintaining internal controls in their programs and administrative activities.
- OMB Circular A-130, Appendix III, 1984: Establishes policy for the management of Federal information resources, as well as the procedures for information systems security
- National Institute of Standards and Technology (NIST 800-14): Generally Accepted Principles and Practices for Securing Information Technology Systems

- National Institute of Standards and Technology (NIST 800-12): An Introduction to Computer Security
- Federal Information Processing Standard 210 (FIPS 210): Personal Identity Verification for Federal Employees and Contractors.
- Federal Information Processing Standard 199 (FIPS 199) Standards for Security Categorization of Federal Information and Information Systems.
- Federal Information Processing Standard 197 (FIPS 197) Advanced Encryption Standard
- The Information Technology Management Reform Act (Clinger-Cohen Act) of 1996 (PL 104-106, Division E) dated August 1996
- National Institute of Standards and Technology (NIST 800-34): Contingency Planning Guide for Information Technology Systems
- National Institute of Standards and Technology (NIST 800-37): Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems
- National Institute of Standards and Technology (NIST 800-40): Creating a Patch and Vulnerability Management Program
- National Institute of Standards and Technology (NIST 800-41): Guidelines on Firewalls and Firewall Policy
- National Institute of Standards and Technology (NIST 800-42): Guideline on Network Security Testing
- National Institute of Standards and Technology (NIST 800-53A): Recommended Security Control Baselines
- National Institute of Standards and Technology (NIST 800-64 Rev2): Security Considerations in the System Development Life Cycle
- Federal Information Processing Standard 102 (FIPS 102): Guidelines for Computer Security Certification and Accreditation dated September 1983

## FINDINGS AND RECOMMENDATIONS

The FISMA evaluation demonstrated that the FLRA's information security posture is not compliant with FISMA requirements, OMB circulars, and NIST guidance. The FLRA has begun the process of performing a Certification and Accreditation (C&A) on the General Support System (GSS) however the GSS was not approved by the designated approving authority (DAA) at the completion of FISMA evaluation testing period. With that being said, the FLRA has begun the process of creating draft IT security policies and procedures which will play a major role in assisting the FLRA in addressing the significant information security weaknesses.

During this evaluation, several FLRA managers and employees expressed their concerns about the organization not having adequate information security. This evaluation confirms the FLRA does not have sufficient information security policies, procedures, and processes to address requirements FISMA requirements, OMB circulars, and NIST guidance. Further, the FLRA has not addressed previous findings and recommendations related to information security. The organization has hired a new CIO that will be serving in a dual role as Chief Information Officer (CIO) and Chief Information Security Officer (CISO), and FLRA senior management plans to support the new CIO in meeting FISMA requirements and changing the information security culture.

We present our specific findings and recommendations in accordance with the requirements documented in NIST publication series:

### 1. Access Control

AC-1 ACCESS CONTROL POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

AC-2 ACCOUNT MANAGEMENT
The organization does not manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization does not review information system accounts [Assignment: organization-defined frequency, at least annually].

AC-3 ACCESS ENFORCEMENT
The information system does not enforce assigned authorizations for controlling access to the system in accordance with applicable policy.

AC-4 INFORMATION FLOW ENFORCEMENT
The information system does not enforce assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

AC-5 SEPARATION OF DUTIES
The information system does not enforce separation of duties through assigned access authorizations.

AC-6 LEAST PRIVILEGE (*the ability to access only such information and resources that are necessary for legitimate purpose).* The information system does not enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS
The information system does not enforce a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] time period. The information system does not automatically [Selection: lock the account/node for an [Assignment: organization-defined time period], and does not delay next login prompt according to [Assignment: organization-defined delay algorithm.]] when the maximum number of unsuccessful attempts is exceeded.

AC-8 SYSTEM USE NOTIFICATION
The information system does not display an approved, system use notification message before granting system access informing potential users: (i) that the user is accessing a U.S. Government information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording. The system use notification message does not provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and does not remain on the screen until the user takes explicit actions to log on to the information system.

AC-9 PREVIOUS LOGON NOTIFICATION
The information system does not notify the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon.

AC-10 CONCURRENT SESSION CONTROL
The information system does not limit the number of concurrent sessions for any user to [Assignment: organization-defined number of sessions].

AC-11 SESSION LOCK
The information system does not prevent further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity, and the session lock does not remain in effect until the user reestablishes access using appropriate identification and authentication procedures.

AC-12 SESSION TERMINATION
The information system does not automatically terminate a remote session after [Assignment: organization-defined time period] of inactivity.

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

The organization does not supervise and review the activities of users with respect to the enforcement and usage of information system access controls.

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
The organization does not identify and document specific user actions that can be performed on the information system without identification or authentication.

AC-15 AUTOMATED MARKING
The information system does not mark output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.

AC-16 AUTOMATED LABELING
The information system does not appropriately label information in storage, in process, and in transmission.

AC-17 REMOTE ACCESS
The organization does not authorize, monitor, and control all methods of remote access to the information system.

AC-18 WIRELESS ACCESS RESTRICTIONS
The organization: (i) does not establish usage restrictions and implementation guidance for wireless technologies; and (ii) does not authorize, monitor, and control wireless access to the information system.

AC-19 ACCESS CONTROL FOR PORTABLE AND MOBILE DEVICES
The organization: (i) does not establish usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and (ii) does not authorize, monitor, and control device access to organizational information systems.

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS
The organization does not establish terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit organization-controlled information using an external information system.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to access control. The organization does have an informal process for granting access. However, during our review we noted that the informal process is not always adhered to.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-116 A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*

**RECOMMENDATION(S):**

We recommend the CIO develop a **robust** access control program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-116 A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*

**MANAGEMENT RESPONSE:**

The CIO agrees with the findings to access control and has a full POA&M to address all findings under the recommendations. In addition nearly all policy findings in this section are addressed within the new Information Security policy handbook.

## 2. Awareness and Training

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

AT-2 SECURITY AWARENESS
The organization does not provide basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [Assignment: organization-defined frequency, at least annually] thereafter.

AT-3 SECURITY TRAINING
The organization does not identify personnel that have significant information system security roles and responsibilities during the system development life cycle, documents those roles and responsibilities, and does not provide appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [Assignment: organization-defined frequency] thereafter.

AT-4 SECURITY TRAINING RECORDS
The organization does not document and monitor individual information system security training activities including basic security awareness training and specific information system security training.

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS
The organization does not establish and maintain contacts with special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations to stay up to date with the latest recommended security practices, techniques, and technologies and to share the latest security-related information including threats, vulnerabilities, and incidents.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to awareness and training. The organization does have an informal process for awareness and training. However, during our review we noted that the informal process is not always adhered to. The organization needs to maintain clear records related to contractors and staff employees who complete awareness and training.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program*

*NIST Special Publication 800-16 Information Technology Security Training Requirements: A Role and Performance-Based Model*

**RECOMMENDATION(S):**

Develop a **robust** awareness and training program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-50 Building an Information Technology Security Awareness and Training Program*

*NIST Special Publication 800-16 Information Technology Security Training Requirements: A Role and Performance-Based Model*

**MANAGEMENT RESPONSE:**

The CIO has satisfied all findings and implemented all recommendations made in this area.

**Audit and Accountability**

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

AU-2 AUDITABLE EVENTS
The organization does not maintain adequate records of failed log in attempts and has not defined unusual activity to track and review. The information system does not generate audit records for the following events: [Assignment: organization-defined auditable events].

AU-3 CONTENT OF AUDIT RECORDS
The information system does not produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

AU-4 AUDIT STORAGE CAPACITY
The organization does not allocate sufficient audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES
The information system does not alert appropriate organizational officials in the event of an audit processing failure and does not take the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].

AU-6 AUDIT MONITORING, ANALYSIS, AND REPORTING
The organization does not regularly review/analyze information system audit records for indications of inappropriate or unusual activity, does not investigate suspicious activity or suspected violations, does not report findings to appropriate officials, and does not take necessary actions.

AU-7 AUDIT REDUCTION AND REPORT GENERATION
The information system does not provide an audit reduction and report generation capability.

AU-8 TIME STAMPS (a sequence of characters, denoting the date and/or time at which a certain event occurred.). The information system does not provide time stamps to indicate the time and date of events for use in audit record generation.

AU-9 PROTECTION OF AUDIT INFORMATION
The information system does not protect audit information and audit tools from unauthorized access, modification, and deletion.

AU-10 NON-REPUDIATION
The information system does not provide the capability to determine whether a given individual took a particular action.

AU-11 AUDIT RECORD RETENTION
The organization does not retain audit records for [Assignment: organization-defined time period] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to audit and accountability.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**RECOMMENDATION(S):**

Develop a **robust** audit and accountability program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**MANAGEMENT RESPONSE:**

The CIO agrees with the findings to Audit and accountability and has a full POA&M to address findings under the recommendations with some acceptations including AU-4 and AU-11.

## 4. Certification, Accreditation, and Security

CA-1 CERTIFICATION, ACCREDITATION, AND SECURITY ASSESSMENT POLICIES AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls.

CA-2 SECURITY ASSESSMENTS
The organization does not conduct an assessment of the security controls in the information system [Assignment: organization-defined frequency, at least annually] 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.

CA-3 INFORMATION SYSTEM CONNECTIONS
The organization does not authorize all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.

CA-4 SECURITY CERTIFICATION
The organization does not conduct an assessment of the security controls in the information system 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.

CA-5 PLAN OF ACTION AND MILESTONES
The organization does not develop and update [Assignment: organization-defined frequency], a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

CA-6 SECURITY ACCREDITATION
The organization does not authorize (i.e., does not accredit) the information system for processing before operations and does not update the authorization [Assignment: organization-defined frequency, at least every three years] or when there is a significant change to the system. A senior organizational official does not sign and approve the security accreditation.

CA-7 CONTINUOUS MONITORING
The organization does not monitor the security controls in the information system on an ongoing basis.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the

process of creating and establishing processes, policy, and procedures related to certification, accreditation, and security. With that being said, the organization is in the process of Certification and Accreditation (C&A) of the General Support System (GSS) which will play a vital role in improving the security posture of the organization.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems*

**RECOMMENDATION(S):**

Develop a **robust** certification, accreditation, and security program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems*

**MANAGEMENT RESPONSE:**

The CIO has satisfied most findings and implemented recommendations made in this area.

## 5. Configuration Management

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

CM-2 BASELINE CONFIGURATION (configuration that can be used as a logical basis for comparison). The organization does not develop, document, and maintain a current baseline configuration of the information system.

CM-3 CONFIGURATION CHANGE CONTROL
The organization does authorize, document, and control changes to the information system.

CM-4 MONITORING CONFIGURATION CHANGES
The organization does not monitor changes to the information system conducting security impact analyses to determine the effects of the changes.

CM-5 ACCESS RESTRICTIONS FOR CHANGE
The organization: (i) does not approve individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) does not generate, retain, and review records reflecting all such changes.

CM-6 CONFIGURATION SETTINGS
The organization: (i) does not establish mandatory configuration settings for information technology products employed within the information system; (ii) does not configure the security settings of information technology products to the most restrictive mode consistent with operational requirements; (iii) does not document the configuration settings; and (iv) does not enforce the configuration settings in all components of the information system.

CM-7 LEAST FUNCTIONALITY
The organization does not configure the information system to provide only essential capabilities and does not specifically prohibit and/or restrict the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited and/or restricted functions, ports, protocols, and/or services].

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY
The organization does not develop, document, and maintain a current inventory of the components of the information system and relevant ownership information.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to configuration management. The organization does have an informal process for configuration management. However, during our review we noted that the informal process is not always adhered to.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**RECOMMENDATION(S):**

Develop a **robust** configuration management program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**MANAGEMENT RESPONSE:**

The FLRA has developed a change risk assessment worksheet and identified a process for change management implementation to include the appropriate change manager based on risk, a full approval process for medium and high risk changes to the environment and has explored the use of an independent technical review board for large implementations of technology. In addition, The FLRA is so significantly behind in nearly all technology to include hardware and software versions, the decision to refresh the entire infrastructure was made prior to FY09. Once upgraded, a baseline of all CI's will be made, categorized and implemented.

## 6. Contingency Planning

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

CP-2 CONTINGENCY PLAN
The organization does not develop and implement a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization do not review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

CP-3 CONTINGENCY TRAINING
The organization does not train personnel in their contingency roles and responsibilities with respect to the information system and does not provide refresher training [Assignment: organization-defined frequency, at least annually].

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES
The organization: (i) does not test and/or exercise the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the plan's effectiveness and the organization's readiness to execute the plan; and (ii) does not review the contingency plan test/exercise results and does not initiate corrective actions.

CP-5 CONTINGENCY PLAN UPDATE
The organization does not review the contingency plan for the information system [Assignment: organization-defined frequency, at least annually] and does not revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.

CP-6 ALTERNATE STORAGE SITE - is a geographically separated site from the primary processing site. The organization does not identify an alternate storage site and does not initiate necessary agreements to permit the storage of information system backup information.

CP-7 ALTERNATE PROCESSING SITE
The organization does not identify an alternate processing site and does not initiate necessary agreements to permit the resumption of information system operations for critical mission/business functions within [Assignment: organization-defined time period] when the primary processing capabilities are unavailable.

CP-8 TELECOMMUNICATIONS SERVICES
The organization does not identify primary and alternate telecommunications services to support the information system and does not initiate necessary agreements to permit the resumption of system operations for critical mission/business functions within [Assignment:

organization-defined time period] when the primary telecommunications capabilities are unavailable.

CP-9 INFORMATION SYSTEM BACKUP
The organization does not conduct backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and does not protect backup information at the storage location.

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
The organization does not employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to contingency planning. The organization does have an informal process for contingency plans. However, during our review we noted that the informal process is not always adhered to.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-34 Contingency Planning Guide for Information Technology Systems*

**RECOMMENDATION(S):**

Develop a **robust** contingency planning program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-34 Contingency Planning Guide for Information Technology Systems*

**MANAGEMENT RESPONSE:**

The FLRA has recently contracted for a plan for a full agency COOP which will satisfy most recommendations found in the audit. In addition, with the most recent IT investments, the remaining findings will implemented by the end of FY10.

## 7. Identification and Authentication

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

IA-2 USER IDENTIFICATION AND AUTHENTICATION
The information system does not uniquely identify and authenticate users (or processes acting on behalf of users).

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION
The information system does not identify and authenticate specific devices before establishing a connection.

IA-4 IDENTIFIER MANAGEMENT
The organization does not manage user identifiers: (i) does not uniquely identify each user; (ii) does not verify the identity of each user; (iii) does not receive authorization to issue a user identifier from an appropriate organization official; (iv) does not issue the user identifier to the intended party; (v) does not disable the user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) does not archive user identifiers.

IA-5 AUTHENTICATOR MANAGEMENT
The organization does not manage information system authenticators: (i) does not define initial authenticator content; (ii) does not establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) does not change default authenticators upon information system installation; and (iv) does not change/refresh authenticators periodically.

IA-6 AUTHENTICATOR FEEDBACK
The information system does not obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION
The information system does not employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to identification and authentication.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-120 DRAFT Recommendation for EAP Methods Used in Wireless Network Access Authentication*

*NIST Special Publication 800-63 Electronic Authentication Guideline*

*NIST Special Publication 800-25 Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*

**RECOMMENDATION(S):**

Develop a **robust** identification and authentication program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-120 DRAFT Recommendation for EAP Methods Used in Wireless Network Access Authentication*

*NIST Special Publication 800-63 Electronic Authentication Guideline*

*NIST Special Publication 800-25 Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*

**MANAGEMENT RESPONSE:**

The CIO disagrees to the findings found in this section. The only access users have into the data enterprise is through the standard Windows 2003 AD. The AD utilizes Kerberos as its authentication mechanism used to verify user or host identity. In Windows Server 2003, the Key Distribution Center selects the strongest encryption type supported by the client. The failure and success of authentication is logged as well.

The CIO agrees that there isn't currently a plan for HSPD12 type crypto graphical module for authentication and in the opinion of the CIO; this would be an acceptable risk.

## 8. Incident Response

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

IR-2 INCIDENT RESPONSE TRAINING
The organization does not train personnel in their incident response roles and responsibilities with respect to the information system and does not provide refresher training [Assignment: organization-defined frequency, at least annually].

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES
The organization does not test and/or exercise the incident response capability for the information system [Assignment: organization-defined frequency, at least annually] using [Assignment: organization-defined tests and/or exercises] to determine the incident response effectiveness and doe not document the results.

IR-4 INCIDENT HANDLING - response by a person or organization to an attack.
The organization does not implement an incident handling capability for security incidents that include preparation, detection and analysis, containment, eradication, and recovery.

IR-5 INCIDENT MONITORING
The organization does not track and document information system security incidents on an ongoing basis.

IR-6 INCIDENT REPORTING
The organization does not promptly report incident information to appropriate authorities.

IR-7 INCIDENT RESPONSE ASSISTANCE
The organization does not provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organization’s incident response capability.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to incident response.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response*

**RECOMMENDATION(S):**

Develop a **robust** incident response program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response*

**MANAGEMENT RESPONSE:**

The CIO agrees that at the time of the audit, the agency did not have a plan or policy dealing with incident response. The Information Assurance policy does address several of the findings and recommendations. This will be addressed in FY10.

## 9. Maintenance

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

MA-2 CONTROLLED MAINTENANCE
The organization does not schedule, perform, document, and review records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

MA-3 MAINTENANCE TOOLS (software and method of controlling a computer from a remote location). The organization does not approve, control, and monitor the use of information system maintenance tools and maintains the tools on an ongoing basis.

MA-4 REMOTE MAINTENANCE
The organization does not authorize, monitor, and control any remotely executed maintenance and diagnostic activities, if employed.

MA-5 MAINTENANCE PERSONNEL
The organization does not allow only authorized personnel to perform maintenance on the information system.

MA-6 TIMELY MAINTENANCE
The organization does not obtain maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to maintenance. The organization does have an informal process for maintenance. However, during our review we noted that the informal process is not always adhered to.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**RECOMMENDATION(S):**

Develop a **robust** maintenance program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**MANAGEMENT RESPONSE:**

The agency has implemented all findings with in this section and now has a robust maintenance plan.

## 10. Media Protection

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

MP-2 MEDIA ACCESS
The organization does not restrict access to information system media to authorized individuals.

MP-3 MEDIA LABELING
The organization: (i) does not affixe external labels to removable information system media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information; and (ii) does not exempt [Assignment: organization-defined list of media types or hardware components] from labeling so long as they remain within [Assignment: organization-defined protected environment].

MP-4 MEDIA STORAGE
The organization does not physically control and securely store information system media within controlled areas.

MP-5 MEDIA TRANSPORT
The organization does not protect and control information system media during transport outside of controlled areas and restricts the activities associated with transport of such media to authorized personnel.

MP-6 MEDIA SANITIZATION AND DISPOSAL
The organization does not sanitize information system media, both digital and non-digital, prior to disposal or release for reuse.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to media protection. The organization does have an informal process for media protection. However, during our review we noted that the informal process is not always adhered to.

### CRITERIA:

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-88 Guidelines for Media Sanitization*

**RECOMMENDATION(S):**

Develop a **robust** media protection program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-88 Guidelines for Media Sanitization*

**MANAGEMENT RESPONSE:**

The CIO disagrees to the findings found in this section. The agency keeps media double locked and provides reasonable security toward storage, transport and access to all media. In addition the deposal of media is addressed in the new policy handbook.

## 11. Physical and Environmental Protection

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

PE-2 PHYSICAL ACCESS AUTHORIZATIONS
The organization does not develop and keep current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and does not issue appropriate authorization credentials. Designated officials within the organization do not review and approve the access list and authorization credentials [Assignment: organization-defined frequency, at least annually].

PE-3 PHYSICAL ACCESS CONTROL
The organization does not control all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and does not verify individual access authorizations before granting access to the facility. The organization does not control access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM
The organization does not control physical access to information system distribution and transmission lines within organizational facilities.

PE-5 ACCESS CONTROL FOR DISPLAY MEDIUM
The organization does not control physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

PE-6 MONITORING PHYSICAL ACCESS
The organization does not monitor physical access to the information system to detect and respond to physical security incidents.

PE-7 VISITOR CONTROL
The organization does not control physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

PE-8 ACCESS RECORDS
The organization does not maintain visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that includes: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and (vii) name and organization of person visited. Designated officials within the organization do not review the visitor access records [Assignment: organization-defined frequency].

PE-9 POWER EQUIPMENT AND POWER CABLING
The organization does not protect power equipment and power cabling for the information system from damage and destruction.

PE-10 EMERGENCY SHUTOFF
The organization does not provide, for specific locations within a facility containing concentrations of information system resources, the capability of shutting off power to any information system component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment.

PE-11 EMERGENCY POWER
The organization does not provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

PE-12 EMERGENCY LIGHTING
The organization does not employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes.

PE-13 FIRE PROTECTION
The organization does not employ and maintain fire suppression and detection devices/systems that can be activated in the event of a fire.

PE-14 TEMPERATURE AND HUMIDITY CONTROLS
The organization does not regularly maintain, within acceptable levels, and monitor the temperature and humidity within the facility where the information system resides.

PE-15 WATER DAMAGE PROTECTION
The organization does not protect the information system from water damage resulting from broken plumbing lines or other sources of water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

PE-16 DELIVERY AND REMOVAL
The organization does not authorize and control information system-related items entering and exiting the facility and does not maintain appropriate records of those items.

PE-17 ALTERNATE WORK SITE
The organization does not employ appropriate management, operational, and technical information system security controls at alternate work sites.

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS
The organization does not position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

PE-19 INFORMATION LEAKAGE
The organization does not protect the information system from information leakage due to electromagnetic signals emanations.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to physical and environmental protection. The organization does have an informal process for physical and environmental protection. However, during our review we noted that the informal process is not always adhered to.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**RECOMMENDATION(S):**

Develop a **robust** physical and environmental protection program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

**MANAGEMENT RESPONSE:**

The CIO agrees to most of the findings listed but specifically disagrees to the findings (PE-4, PE-5, and PE-6). Physical access, control for transmission medium and display medium are all provided with reasonable provisions.

The agency recently invested in an access control system for physical access to the IT datacenter which will record and control access. This is planned to be installed within 3 months

The CIO disagrees to PE-9, PE-10, and PE-11. All power distribution is provided to the IT enterprise with surge and battery (emergency power) provisions.

The CIO disagrees to PE-16. All delivery and removal is controlled by a long standing policy

The CIO disagrees to PE-18; the location of the datacenter was determined to be the best location for both efficiency and hazards.

The CIO disagrees to PE-19. This is an acceptable risk as TEMPEST emissions protection is only required for classification of sensitive or above information classifications.

## 12. Planning

PL-1 SECURITY PLANNING POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

PL-2 SYSTEM SECURITY PLAN
The organization does not develop and implement a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organization do not review and approve the plan.

PL-3 SYSTEM SECURITY PLAN UPDATE

The organization does not review the security plan for the information system [Assignment: organization-defined frequency, at least annually] and do not revise the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.

PL-4 RULES OF BEHAVIOR
The organization does not establish and make readily available to all information system users, a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization does not receive signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information.

PL-5 PRIVACY IMPACT ASSESSMENT
The organization does not conduct a privacy impact assessment on the information system in accordance with OMB policy.

PL-6 SECURITY-RELATED ACTIVITY PLANNING
The organization does not plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to planning.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**RECOMMENDATION(S):**

Develop a **robust** planning program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**MANAGEMENT RESPONSE:**

The CIO agrees with the findings to Planning and has a full POA&M to address all findings under the recommendations. In addition nearly all policy findings in this section are addressed within the new Information Security policy handbook.

## 13. Personnel Security

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

PS-2 POSITION CATEGORIZATION
The organization does not assign a risk designation to all positions and does not establish screening criteria for individuals filling those positions. The organization does not review and revise position risk designations [Assignment: organization-defined frequency].

PS-3 PERSONNEL SCREENING
The organization does not screen individuals requiring access to organizational information and information systems before authorizing access.

PS-4 PERSONNEL TERMINATION
The organization, upon termination of individual employment, does not terminate information system access, does not conduct exit interviews, does not retrieve all organizational information system-related property, and does not provide appropriate personnel with access to official records created by the terminated employee that are stored on organizational information systems.

PS-5 PERSONNEL TRANSFER
The organization does not review information systems/facilities access authorizations when personnel are reassigned or transferred to other positions within the organization and does not initiate appropriate actions.

PS-6 ACCESS AGREEMENTS
The organization does not complete appropriate signed access agreements for individuals requiring access to organizational information and information systems before authorizing access and does not review/update the agreements [Assignment: organization-defined frequency].

PS-7 THIRD-PARTY PERSONNEL SECURITY
The organization does not establish personnel security requirements including security roles and responsibilities for third-party providers and does not monitor provider compliance.

PS-8 PERSONNEL SANCTIONS

The organization does not employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to personnel security. The organization does have an informal process for personnel security. However, during our review we noted that the informal process is not always adhered to.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**RECOMMENDATION(S):**

Develop a **robust** personnel security program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**MANAGEMENT RESPONSE:**

The CIO disagrees with PS-3. No one is granted access to IT resources within the FLRA without expressed permission from agency supervisors. The CIO agrees to all other findings; and they are addressed within the new Information Security policy handbook.

## 14. Risk Assessment

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

RA-2 SECURITY CATEGORIZATION
The organization does not categorize the information system and the information processed, stored, or transmitted by the system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance and does not document the results

(including supporting rationale) in the system security plan. Designated senior-level officials within the organization do not review and approve the security categorizations.

RA-3 RISK ASSESSMENT
The organization does not conduct assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).

RA-4 RISK ASSESSMENT UPDATE
The organization does not update the risk assessment [Assignment: organization-defined frequency] or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.

RA-5 VULNERABILITY SCANNING
The organization does not scan for vulnerabilities in the information system [Assignment: organization-defined frequency] or when significant new vulnerabilities potentially affecting the system are identified and reported.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to risk assessment. The organization does have an informal process for risk assessment. However, during our review we noted that the informal process is not always adhered to.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication SP 800-30 Risk Management Guide for Information Technology Systems*

**RECOMMENDATION(S):**

Develop a **robust** risk assessment program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**MANAGEMENT RESPONSE:**

The CIO agrees to these findings. The CIO agrees to all other findings which are addressed within the new Information Security policy handbook.

## 15. System and Services Acquisition

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

SA-2 ALLOCATION OF RESOURCES
The organization does not determine, document, and allocate as part of its capital planning and investment control process, the resources required to adequately protect the information system.

SA-3 LIFE CYCLE SUPPORT
The organization does not manage the information system using a system development life cycle methodology that includes information security considerations.

SA-4 ACQUISITIONS
The organization does not include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, Executive Orders, directives, policies, regulations, and standards.

SA-5 INFORMATION SYSTEM DOCUMENTATION
The organization does not obtain, protect as required, and make available to authorized personnel, adequate documentation for the information system.

SA-6 SOFTWARE USAGE RESTRICTIONS
The organization does not comply with software usage restrictions.

SA-7 USER INSTALLED SOFTWARE
The organization does not enforce explicit rules governing the installation of software by users.

SA-8 SECURITY ENGINEERING PRINCIPLES
The organization does not design and implement the information system using security engineering principles.

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES
The organization: (i) does not require that providers of external information system services employ adequate security controls in accordance with applicable laws, Executive Orders,

directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) does not monitor security control compliance.

SA-10 DEVELOPER CONFIGURATION MANAGEMENT
The organization does not require that information system developers create and implement a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and does not provide documentation of the plan and its implementation.

SA-11 DEVELOPER SECURITY TESTING
The organization does not require that information system developers create a security test and evaluation plan, implement the plan, and document the results.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to system and services acquisition. The organization does have an informal process for system and services acquisition. However, during our review we noted that the informal process is not always adhered to.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-23 Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*

**RECOMMENDATION(S):**

Develop a **robust** system and services acquisition program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-23 Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*

**MANAGEMENT RESPONSE:**

The CIO agrees to these findings. The agency has recently put into place a full refresh life cycle support to ensure all hardware and software is updated. In addition, the agency does follow the OMB guidance on Federal Acquisition of Foreign Supplies and Services

## 16. System and Communications Protection

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

SC-2 APPLICATION PARTITIONING
The information system does not separate user functionality (including user interface services) from information system management functionality.

SC-3 SECURITY FUNCTION ISOLATION
The information system does not isolate security functions from non-security functions.

SC-4 INFORMATION REMNANCE
The information system does not prevent unauthorized and unintended information transfer via shared system resources.

SC-5 DENIAL OF SERVICE PROTECTION
The information system does not protect against or limit the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list].

SC-6 RESOURCE PRIORITY
The information system does not limit the use of resources by priority.

SC-7 BOUNDARY PROTECTION
The information system does not monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.

SC-8 TRANSMISSION INTEGRITY
The information system does not protect the integrity of transmitted information.

SC-9 TRANSMISSION CONFIDENTIALITY
The information system does not protect the confidentiality of transmitted information.

SC-10 NETWORK DISCONNECT

The information system does not terminate a network connection at the end of a session or after [Assignment: organization-defined time period] of inactivity.

SC-11 TRUSTED PATH
The information system does not establish a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and re-authentication].

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT
When cryptography is not required and employed within the information system, the organization does not establish and manage cryptographic keys using automated mechanisms with supporting procedures or manual procedures.

SC-13 USE OF CRYPTOGRAPHY - the practice and study of hiding information.
For information requiring cryptographic protection, the information system does not implement cryptographic mechanisms that comply with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

SC-14 PUBLIC ACCESS PROTECTIONS
The information system does not protect the integrity and availability of publicly available information and applications.

SC-15 COLLABORATIVE COMPUTING
The information system does not prohibit remote activation of collaborative computing mechanisms and does not provide an explicit indication of use to the local users.

SC-16 TRANSMISSION OF SECURITY PARAMETERS
The information system does not reliably associate security parameters with information exchanged between information systems.

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES ( a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates). The organization does not issue public key certificates under an appropriate certificate policy and does not obtain public key certificates under an appropriate certificate policy from an approved service provider.

SC-18 MOBILE CODE
The organization: (i) does not establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) does not authorize, monitor, and control the use of mobile code within the information system.

SC-19 VOICE OVER INTERNET PROTOCOL
The organization: (i) does not establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) does not authorize, monitor, and control the use of VoIP within the information system.

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
The information system that provides name/address resolution service does not provide additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries.

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)
The information system that provides name/address resolution service for local clients does not perform data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE
The information systems that collectively provide name/address resolution service for an organization are not fault tolerant and do not implement role separation.

SC-23 SESSION AUTHENTICITY
The information system does not provide mechanisms to protect the authenticity of communications sessions.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to system and communications protection.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*NIST Special Publication 800-13 Telecommunications Security Guidelines for Telecommunications Management Network*

**RECOMMENDATION(S):**

Develop a **robust** system and communications protection program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**MANAGEMENT RESPONSE:**

The CIO agrees with the findings to System and Security Protection and has a full POA&M to address all findings under the recommendations. All policy findings in this section are addressed within the new Information Security policy handbook. In addition the agency has begun the process for compliance to the Trusted Internet Connection (TIC) and the DHS Einstein program.

## 17. System and Information Integrity

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES
The organization does not develop, disseminate, and periodically review/update: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

SI-2 FLAW REMEDIATION
The organization does not identify, report, and correct information system flaws.

SI-3 MALICIOUS CODE PROTECTION
The information system does not implement malicious code protection.

SI-4 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES
The organization does not employ tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.

SI-5 SECURITY ALERTS AND ADVISORIES
The organization does not receive information system security alerts/advisories on a regular basis, does not issue alerts/advisories to appropriate personnel, and does not take appropriate actions in response.

SI-6 SECURITY FUNCTIONALITY VERIFICATION
The information system does not verify the correct operation of security functions [Selection (one or more): upon system startup and restart, upon command by user with appropriate privilege, periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): does not notify system administrator, does not shut the system down, and does not restart the system] when anomalies are discovered.

SI-7 SOFTWARE AND INFORMATION INTEGRITY
The information system does not detect and protect against unauthorized changes to software and information.

SI-8 SPAM PROTECTION

The information system does not implement spam protection.

SI-9 INFORMATION INPUT RESTRICTIONS
The organization does not restrict the capability to input information to the information system to authorized personnel.

SI-10 INFORMATION ACCURACY, COMPLETENESS, VALIDITY, AND AUTHENTICITY
The information system does not check information for accuracy, completeness, validity, and authenticity.

SI-11 ERROR HANDLING
The information system does not identify and handles error conditions in an expeditious manner without providing information that could be exploited by adversaries.

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION
The organization does not handle and retain output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to system and information integrity.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**RECOMMENDATION(S):**

Develop a **robust** system and information integrity program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

**MANAGEMENT RESPONSE:**

The CIO disagrees with SI-2, SI-8. The agency employs a helpdesk to identify and remediate interactions, incidences, and problems for identified flaws. In addition, the agency utilizes the industries best SPAM protection and has done so for several years.

The CIO also determines some of these findings to be out of scope and unreasonable considering the level and classification of the information within the organization.

Most policy findings in this section are addressed within the new Information Security policy handbook.

## 18. Privacy Protection

M-07-16 SAFEGUARDING AGAINST AND REPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORAMTION The organization does not safeguarding personally identifiable information in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 (FISMA) and the Privacy Act of 1974.

Specifically we found that: During our interviews with the organization information technology staff we were able to determine that the organization is very immature in the process of creating and establishing processes, policy, and procedures related to privacy protection. The organization has begun to encrypting laptop for FLRA however a robust information privacy plan and approach has not been established.

**CRITERIA:**

*NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*

*OMB - M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (August 20, 2009) (25 pages, 178 kb)*

*OMB - Recommendations for Identity Theft Related Data Breach Notification*

*OMB - M-06-16, Protection of Sensitive Agency Information*

*OMB - M-06-15, Safeguarding Personally Identifiable Information*

*OMB - M-06-06, Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12*

**RECOMMENDATION(S):**

Develop a **robust** privacy program in accordance with *NIST Special Publication 800-53 Revision 2 Recommended Security Controls for Federal Information Systems*

*NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems Building Effective Security Assessment Plans*
*OMB - M-09-29, FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (August 20, 2009) (25 pages, 178 kb)*

*OMB - Recommendations for Identity Theft Related Data Breach Notification*

*OMB - M-06-16, Protection of Sensitive Agency Information*

*OMB - M-06-15, Safeguarding Personally Identifiable Information*

*OMB - M-06-06, Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12*

**MANAGEMENT RESPONSE:**

The FLRA CIO disagrees with the auditor in that the agency exercises reasonable provisions to protect PII both "in motion" and "at-rest". In addition, the agency does not have high-level PII within its enterprise requiring involved protection measures. The agency does to a large degree encrypt electronic data in compliance with FIPS199 for both mobile devices and session traffic.

The FLRA CIO and SAOP believe FLRA does need to get a written policy on PII in place. FLRA is starting to work on that. Also, from a Privacy Act perspective, although we do have a published list of our Privacy Act systems of records, and these are all human resource records, it is in need of an update.

**Control Families Definitions**

Access Control – provide a technical means of controlling what information users can utilize, the programs they can run, and the modifications they can make.

Awareness and Training – improving awareness of the need to protect system resources, developing skills and knowledge so computer users can perform their jobs more securely, and building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

or:

Awareness stimulates and motivates those being trained to care about security and to remind them of important security practices. Training teaches people the skills that will enable them to perform their jobs more securely.

Audit and Accountability – review and analysis of management, operational, and technical controls.

Certification, Accreditation and Security – formal testing of the security safeguards implemented in the computer system to determine whether they meet applicable requirements and specifications and the formal authorization by the accrediting (management) official for system operation and an explicit acceptance of risk.

Configuration Management – the process of keeping track of changes to the system and, if needed, approving them.

Contingency Planning – the initial actions taken to protect lives and limit damage, the steps that are taken to continue support for critical functions, and the return to normal operations.

Cryptography – encryption of data; can be used to provide many security services, such as electronic signatures and ensuring that data has not been modified.

Identification and Authentication – the portion of access control that prevents unauthorized people (or unauthorized processes) from entering a computer system.

Incident Response – the portion of contingency planning that responds to malicious technical threats.

Maintenance – the system is almost always modified by the addition of hardware and software and by numerous other events

Media Protection – a variety of measures to provide physical and environmental protection and accountability for tapes, diskettes, printouts, and other media.

Physical and Environmental Protection – measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.

Planning – used to help ensure that security is addressed in a comprehensive manner throughout a system's life cycle.

Personnel Security – involves those measures taken to safeguard a company's employees and those coming to a place of business either for business reasons or as guests.

Risk Assessment – the process of analyzing and interpreting risk; entails determining the assessment's scope and methodology, collecting and analyzing data, and interpreting the risk analysis results.

System and Services Acquisition – a detailed list of functional, security, and system requirements; developing vendor selection criteria; and reviewing contracts and licensing agreements.

System and Communications Protection – provides protection to information system and communication needed to meet the government and industry standards and requirements.

System and Information Integrity – Information has integrity when it is timely, accurate, complete, and consistent. However, computers are unable to provide or protect all of these qualities.

**Common Terms and Definitions**

Accreditation
[FIPS 200, NIST SP 800-37]
The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

Accreditation Boundary
[NIST SP 800-37]
All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.

Accreditation Package
The evidence provided to the authorizing official to be used in the security accreditation decision process. Evidence includes, but is not limited to: (i) the system security plan; (ii) the assessment results from the security certification; and (iii) the plan of action and milestones.

Accrediting Authority - See Authorizing Official.

Adequate Security
[OMB Circular A-130, Appendix III]
Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Agency - See Executive Agency.

Application

[OMB Circular A-130, Appendix III]
The use of information resources (information and information technology) to satisfy a specific set of user requirements.

Assessment Method
A focused activity or action employed by an assessor for evaluating a particular attribute of a security control.

Assessment Procedure
A set of activities or actions employed by an assessor to determine the extent to which a security control is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Authentication
[FIPS 200]
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authenticity
The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.

Authorize Processing - See Accreditation.

Authorization - See Accreditation.
Authorize Processing - See Accreditation.

Authorizing Official
[FIPS 200, NIST SP 800-37]
Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority.

Authorizing Official Designated Representative
Individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system.

Availability
[44 U.S.C., Sec. 3542]
Ensuring timely and reliable access to and use of information.

Backup
A copy of files and programs made to facilitate recovery if necessary.

Boundary Protection
Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of

boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

Boundary Protection Device
A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) monitors and controls communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications. Boundary protection devices include such components as proxies, gateways, routers, firewalls, guards, and encrypted tunnels.

Business Continuity Plan (BCP)
The documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.
Business Impact Analysis (BIA): An analysis of an information technology (IT) system's requirements, processes, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.

Business Recovery/Resumption Plan (BRP)
The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption has occurred.
Cold Site: A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.

Certification
[FIPS 200, NIST SP 800-37]
A comprehensive assessment of the management, operational and technical security controls in an information system, made in support of security accreditation, 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.

Certification Agent
[NIST SP 800-37]
The individual, group, or organization responsible for conducting a security certification.
Certification Practice Statement
A statement of the practices that a Certification Authority employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in a certificate policy or requirements specified in a contract for services).

Chief Information Officer
[PL 104-106, Sec. 5125 (b)]
Agency official responsible for:
(i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;

(ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and
(iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Commodity Service
An information system service (e.g., telecommunications service) provided by a commercial service provider typically to a large and diverse set of consumers. The organization acquiring and/or receiving the commodity service possesses limited visibility into the management structure and operations of the provider and while the organization may be able to negotiate service-level agreements, the organization is typically not in a position to require that the provider implement specific security controls.

Common Carrier
In a telecommunications context, a telecommunications company that holds itself out to the public for hire to provide communications transmission services. Note: In the United States, such companies are usually subject to regulation by federal and state regulatory commissions.

Common Security Control
[NIST SP 800-37]
Security control that can be applied to one or more agency information systems and has the following properties: (i) the development, implementation, and assessment of the control can be assigned to a responsible official or organizational element (other than the information system owner); and (ii) the results from the assessment of the control can be used to support the security certification and accreditation processes of an agency information system where that control has been applied.

Compensating Security Controls
The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.

Computer
A device that accepts digital data and manipulates the information based on a program or sequence of instructions for how data is to be processed.
Contingency Plan: Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

Confidentiality
[44 U.S.C., Sec. 3542]
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control
[CNSS Inst. 4009]

Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.

Contingency Planning - See Contingency Plan.

Continuity of Operations Plan (COOP)
A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.

Continuity of Support Plan
The documentation of a predetermined set of instructions or procedures mandated by Office of Management and Budget (OMB) A-130 that describe how to sustain major applications and general support systems in the event of a significant disruption.

Controlled Area
Any area or spaces for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

Countermeasures
[CNSS Inst. 4009]
Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

Disaster Recovery Plan (DRP)
A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

Disruption
An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Executive Agency
[41 U.S.C., Sec. 403]
An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

External Information System (or Component)
An information system or component of an information system that is outside of the accreditation boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External Information System Service

An information system service that is implemented outside of the accreditation boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system).

External Information System Service Provider
A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.

Federal Enterprise Architecture
[FEA Program Management Office]
A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.

Federal Information System
[40 U.S.C., Sec. 11331]
An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

General Support System
[OMB Circular A-130, Appendix III]
An interconnected information resource under the same direct management controls that shares common functionality. It usually includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Guard (System)
[CNSS Inst. 4009, Adapted]
A mechanism limiting the exchange of information between information systems or subsystems.

High-Impact System
[FIPS 200]
An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.

Hot Site
A fully operational off-site data processing facility equipped with hardware and system software to be used in the event of a disaster.

Incident
[FIPS 200]
An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or

transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Incident Response Plan
The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's IT systems(s).

Industrial Control System
An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.

Information
[FIPS 199]
An instance of an information type.

Information Owner
[CNSS Inst. 4009]
Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Resources
[44 U.S.C., Sec. 3502]
Information and related resources, such as personnel, equipment, funds, and information technology.

Information Security
[44 U.S.C., Sec. 3542]
The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Policy
[CNSS Inst. 4009]
Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information System
[44 U.S.C., Sec. 3502]
[OMB Circular A-130, Appendix III]
A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Owner (or Program Manager)
[CNSS Inst. 4009, Adapted]

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information System Security Officer
[CNSS Inst. 4009, Adapted]
Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program.

Information Technology
[40 U.S.C., Sec. 1401]
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Information Type
[FIPS 199]
A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Integrity
[44 U.S.C., Sec. 3542]
Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Label - See Security Label.

Line of Business
The following OMB-defined process areas common to virtually all federal agencies: Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure.

Local Access
Access to an organizational information system by a user (or an information system) communicating through an internal organization-controlled network (e.g., local area network) or directly to a device without the use of a network.

Low-Impact System
[FIPS 200]

An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

Major Application
[OMB Circular A-130, Appendix III]
An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

Major Information System
[OMB Circular A-130]
An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

Malicious Code
[CNSS Inst. 4009]
[NIST SP 800-61]
Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Malware - See Malicious Code.

Management Controls
[FIPS 200]
The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

Media
[FIPS 200]
Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Media Access Control Address
A hardware address that uniquely identifies each component of an IEEE 802-based network. On networks that do not conform to the IEEE 802 standards but do conform to the OSI Reference Model, the node address is called the Data Link Control (DLC) address.

Media Sanitization
[NIST SP 800-88]
A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Minor Application
An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

Mobile Code
Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

Mobile Code Technologies
Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).

Mobile Site
A self-contained, transportable shell custom-fitted with the specific IT equipment and telecommunications necessary to provide full recovery capabilities upon notice of a significant disruption.

Moderate-Impact System
[FIPS 200]
An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.
National Security Emergency Preparedness Telecommunications Services
[47 C.F.R., Part 64, App A]
Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.

National Security Information
Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

National Security System
[44 U.S.C., Sec. 3542]
Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— (i) the

function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Non-repudiation
[CNSS Inst. 4009]
Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

Operational Controls
[FIPS 200]
The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

Organization
[FIPS 200]
A federal agency or, as appropriate, any of its operational elements

Plan of Action and Milestones
[OMB Memorandum 02-01]
A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Potential Impact
[FIPS 199]
The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.

Privacy Impact Assessment
[OMB Memorandum 03-22]
An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privileged Function
A function executed on an information system involving the control, monitoring, or administration of the system.

Privileged User
[CNSS Inst. 4009]
Individual who has access to system control, monitoring, or administration functions (e.g., system administrator, information system security officer, maintainer, system programmer)

Protective Distribution System
Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.

Reciprocal Agreement
An agreement that allows two organizations to back up each other.

Records
The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

Remote Access
Access to an organizational information system by a user (or an information system) communicating through an external, non-organization-controlled network (e.g., the Internet).

Remote Maintenance
Maintenance activities conducted by individuals communicating through an external, non-organization-controlled network (e.g., the Internet)

Risk
[FIPS 200]
The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment
[NIST SP 800-30, Adapted]
The process of identifying risks to agency operations (including mission, functions, image or reputation), agency assets or individuals arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in place security controls.

Risk Management
[FIPS 200]
The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the

implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Safeguards
[CNSS Inst. 4009, Adapted]
Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls, and countermeasures.

Scoping Guidance
Provide organizations with specific policy/regulatory-related, technology-related, physical infrastructure-related, operational/environmental-related, public access-related, scalability-related, common security control-related, and security objective-related considerations on the applicability and implementation of individual security controls in the control baseline.

Security Authorization - See Accreditation
Security Accreditation - See Accreditation
Security Category
[FIPS 199]
The characterization of information or a information systems based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Security Controls
[FIPS 199]
The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Control Baseline
[FIPS 200]
The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

Security Control Enhancements
Statements of security capability to: (i) build in additional, but related, functionality to a basic control; and/or (ii) increase the strength of a basic control.

Security Functions
The hardware, software, and firm ware of the information system responsible for supporting and enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

Security Impact Analysis
[NIST SP 800-37]

The analysis conducted by an agency official, often during the continuous monitoring phase of the security certification and accreditation process, to determine the extent to which changes to the information system have affected the security posture of the system.

Security Incident - See Incident

Security Label
Explicit or implicit marking of a data structure or output media associated with an information system representing the FIPS 199 security category, or distribution limitations or handling caveats of the information contained therein.

Security Objective
[FIPS 199]
Confidentiality, integrity, or availability

Security Perimeter - See Accreditation Boundary

Security Plan - See System Security Plan

Security Requirements
[FIPS 200]
Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.
Senior Agency

Senior Agency Information Security Officer
[44 U.S.C., Sec. 3544]
Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.

Spyware
Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code

Subsystem
A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific function

System
A generic term used for briefness to mean either a major application or a general support system. See also Information System.

System Development Life Cycle

The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

System-specific Security Control
[NIST SP 800-37]
A security control for an information system that has not been designated as a common security control

System Security Plan
[NIST SP 800-18, Rev 1]
Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Tailoring
The process by which a security control baseline selected in accordance with the FIPS 199 security categorization of the information system is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls, where allowed.
Tailored Security Control Baseline
Set of security controls resulting from the application of the tailoring guidance to the security control baseline.

Technical Controls
[FIPS 200]
The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Threat
[CNSS Inst. 4009, Adapted]
Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Agent - See Threat Source

Threat Assessment
[CNSS Inst. 4009]
Formal description and evaluation of threat to an information system

Trusted Path
A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by un-trusted software.

Threat Source
[FIPS 200]
The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability; synonymous with threat agent.

User
[CNSS Inst. 4009]
Individual or (system) process authorized to access an information system.

User Representative
An individual that represents the operational interests of the user community and serves as the liaison for that community throughout the system development life cycle of the information system

Vulnerability
[CNSS Inst. 4009, Adapted]
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

Vulnerability Assessment
[CNSS Inst. 4009]
Formal description and evaluation of the vulnerabilities in an information system
Special Publication 800-53, Revision 2 Recommended Security Controls for Federal Information Systems

Warm Site
An environmentally conditioned workspace that is partially equipped with IT and telecommunications equipment to support relocated IT operations in the event of a significant disruption