DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

SECURITY TEST AND EVALUATION (ST&E) TEST PLAN TEMPLATE

Version 1.0

April 2005

[SYSTEM NAME]
[Organization]

[DATE PREPARED]

Prepared by:

Preparing Organization

TABLE OF CONTENTS

[SYSTEM NAME]
SECURITY TEST AND EVALUATION REVIEW/APPROVAL SHEET

System Owner:		
Name:	**Signature**	**Date**

Security Officer:		
Name:	**Signature**	**Date**

Security Reviewer:		
Name:	**Signature**	**Date**

INTRODUCTION

A Security Testing and Evaluation (ST&E) is essential to the certification and accreditation (C&A) process. An ST&E is used to determine the system's compliance with defined security requirements where the correctness and effectiveness of the security controls implementing the security requirements are tested. The ST&E Results Report documents which of the security controls are effective and which security controls are not effective or fully implemented. The security controls that are not effective or fully implemented are documented in a Risk Assessment, which defines the residual risk for the system prior to mitigation and after appropriate risk mitigation has occurred. The Designated Approving Authority (DAA) will then determine the acceptable level of risk based on the agency's requirements, while using the Risk Assessment and certification package to issue an Interim Authority to Operate accreditation, or no accreditation of the system.

An ST&E can be conducted on a developmental system or an operational system. Depending on the stage of the life cycle that the system is in, the ST&E process and test methods may vary. However, a minimal set of security requirements is essential for an ST&E. As referenced in its *Certification and Accreditation Process Overview*, Department of Housing and Urban Development has adopted National Institute of Standards and Technology (NIST) Special Publication 800-53: *Recommended Security Controls for Federal Information Systems* as its minimum security baseline. Depending on the information sensitivity, confidentiality, integrity, or availability of the information, and the mission criticality of the system undergoing testing, and the manner in which the system has been implemented, the minimal set of security requirements may need to be augmented. This is normally through risk assessment of the system.

The information sensitivity and mission criticality of the system can be determined by using the Department of Housing and Urban Development's *IT System Certification and Accreditation Inventory Guide*, April 2005:

- Security controls specific to the Department (policy-driven).
- Security controls specific to, but not limited to, hardware, software, operating system, applications and databases on the system (technology-driven).
- Security controls based on the increased levels of concern for confidentiality, integrity, and availability (sensitivity-driven).
- Security controls based on the internal or external exposure and risk based decisions (exposure/risk-driven).

For example, a system with a high information sensitivity rating that is mission critical should be considered for a comprehensive test to include augmenting the minimal security requirements with all four types of security control whereby the minimal security requirements would satisfy a test for a system with a low information sensitivity that is not mission critical. Additionally, depending on the information sensitivity and criticality of the system, the intensity of verification and validation should be considered, which may range from a simple minimum security checklist

for low, non-critical systems to detailed ST&E and penetration testing for highly sensitive and critical systems.

1.0 Document Overview

This document reports the results of the Security Test & Evaluation (ST&E) activities for the [System Name]. The ST&E follows the requirements set forth by the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, and additional risk-based controls documented in the [System Name] risk assessment. The results outlined in this document include the potential vulnerabilities, and identification and validation of security control.

1.1. Purpose

The purpose of the security testing is to verify the compliance with security policy guidelines and evaluation their effectiveness against anticipated threats. The document identifies the system to be tested, the approach used for testing, the testing team, and the results of the testing activity.

1.2. Objectives

The overall objective of the ST&E is to ensure that a comprehensive testing activity is identified that covers all appropriate security requirements, involves all necessary individuals, and ultimately provides the information needed to support the Certification & Accreditation (C&A) process.

1.3. Memoranda of Understanding (MOUs)

The current MOUs applicable to [System Name] are identified in Table 1-1.

Table 1-1. Memoranda of Understanding

Agreement	Date Initiated	Expiration Date

1.4. Responsible Organizations/Personnel

The organizations and personnel responsible for the security of the [System Name] are identified in Table 1-2.

Table 1-2. System Security Management Personnel

Function	Organization	Name
Designated Approving Authority (DAA)	Insert title	Insert name
Information System Security Certifier (ISSC)	Insert title	Insert name
Information System Security Manager (ISSM)	Insert title or N/A	Insert name or N/A
Information System Security Officer (ISSO)	Insert title	Insert name
System Owner	Insert title	Insert name

1.5. Assumptions

- The system operational site processes sensitive but unclassified information as well as non-sensitive commercial message traffic.
- The system will be minimally evaluated against the requirements identified in NIST SP 800-53 and augmented with policy-driven, technology-driven, sensitivity driven, and exposure/risk-driven security controls as applicable.
- The scope of testing will include compliance with applicable security requirements, where the validation and verification intensity will vary, given the information sensitivity and mission criticality.
- All required documents, key personnel, and system access must be available to the test team in a timely manner to meet the testing schedule.

1.6. Scope

All components of the system identified in the [System Name] Security Plan, dated MM/DD/YYYY will be tested and evaluated as part of this ST&E.

Excluded from this assessment XXXXXXX network perimeter security function and components, all of which will be described within their respective certifications.

2.0 ST&E Requirements

The criteria against which the system will be tested were obtained from the NIST SP 800-53. The test categories are listed in the Table 2-1:

Table 2-1. System Security Test Categories

MANAGEMENT CONTROLS
Risk Assessment
Planning
Systems and Services Acquisition
Certification, Accreditation, and Security Assessments
OPERATIONAL CONTROLS
Personnel Security
Physical and Environmental Protection
Contingency Planning
Configuration Management
Maintenance
System and Information Integrity
Media Protection
Incident Response
Awareness and Training
TECHNICAL CONTROLS
Identification and Authentication
Access Controls
Audit and Accountability
System and Communications Protection

3.0 ST&E Approach

3.1. General Approach

The basic approach to the ST&E is to determine how well the system supports the established requirements and to identify any unsupported requirements or requirements that are not fully supported. The security requirements consist of those items identified in NIST SP 800-26 in addition to specific Department of Housing and Urban Development (HUD) requirements.

The methods for testing and evaluating include:

- **Demonstration** – the evaluation by operation, movement, or adjustment under a specific condition to determine the capability to satisfy a stated requirement.
- **Inspection** – the physical examination or review of the feature, such as review of a configuration file or software version number/patch level.
- **Test** – the collection, analysis, and evaluation through systematic hands-on measurement under appropriate conditions.

Testing techniques will consider threat and vulnerability information from both government and industry sources to evaluate a comprehensive range of attack methods. Emphasis is placed on the existence of security controls as well as evidence of security as an integral part of the business environment. Problems that are identified during the testing activity can be immediately corrected or may be identified as items of concern, which are discussed in detail in the mitigation plan.

3.2. The System Operational Service Approach

Because the system provides an operational service, the test approach for testing will use a non-intrusive set of tests. The security testing will include manual review of a sampling of critical files from the live system components and review of procedures. The requirements that will be addressed on the operational system will be annotated on the Plan of Action and Milestones. This test approach has been designed to avoid any possible disruption to ongoing activities. Tests will be conducted in close coordination with individuals familiar with administration of the system to draw on their expertise in system operation and to identify any potential for system disruption.

3.3. System Tests and Protocols

The testing of the information system's security features may range from a series of formal tests to a penetration test of the information system. The following types of test plans and results may need to be reviewed and the results/recommendations from these tests summarized in the Security Test Report. The following list is not all-inclusive.

- **Operational Test (OT)** – Demonstrates the system is operationally effective and operationally suitable for use and that the system is ready to be certified and accredited. These tests focus on demonstrating that operational requirements have been met and that a mitigation plan has been developed and accepted to resolve deficiencies.

- **Penetration Test (PT) -** The evaluator attempts to circumvent the security features of a system to gain access. **NOTE:** Penetration testing on HUD information systems must have advanced coordination and formal authorization with the DAA for the line of business or staff office that owns the system, the information owner (if not the same as the system owner), and the Office of Chief Counsel. If the penetration test could impact one or more systems for which other DAAs are responsible, then coordination must include all affected DAAs. In addition, all personnel participating in the testing should meet background investigation personnel requirements.

- **System Test (ST)** – A series of tests designed to verify that a system meets its specified requirements. Subsets of the system test are development tests, operational tests, environmental tests and personnel acceptance tests. Each must verify satisfaction of all requirements associated with a system. Results of this testing are included in Appendix A (Test Procedures) and Appendix B (Document Evidence).

- **Vulnerability Test (VT)** – The evaluator attempts to identify security vulnerabilities that may compromise the system by using approved HUD vulnerability scanning method. These may include, but are not limited to, port scans, available services, password checks, and system patches. See vulnerability scan results (Appendix C).

3.4. Schedule

Testing will be accomplished on insert inclusive dates of testing.

4.0 Team Composition/Roles & Responsibilities

4.1. Identification of Team

The ST&E team will be composed of technically competent individuals who have expertise in the discipline they are evaluating. Where required, appropriate team members will have knowledge of how the information flows by function and have an understanding of how the various subsystems support the total configuration and the potential security vulnerabilities of the configuration. In addition, they will be familiar with the security architecture and its impact on the specific evaluations to be conducted. The team will be composed of the individuals identified in Table 3-1.

Table 3-1. Test Team Members

Function/Area Of Expertise	Name	Organization
Test Sponsor/Information System Security Certifier (ISSC)		
Certifying Agent/Test Director		
Other test team members		

4.2. Roles and Responsibilities

Test Sponsor/Information System Security Certifier (ISSC): The responsibilities for the ST&E effort will be to:

- Monitor and approve all testing activities.
- Review and approve test reports.
- Certify that the test results of the system are accurate as stated in the Security Test Report and provide this certification in writing to the accrediting authority.

Certifying Agent/Test Director: The responsibilities for the ST&E effort will be to:

- Assist in selecting, preparing, and approving the test procedures to be used during the Security Test effort.
- Direct the Security Test and coordinate schedule changes.
- Develop the Security Test report.

Test Team Members: The responsibilities for the ST&E effort will be to:

- Assist Test Director in selecting, preparing, and approving the test procedures to be used during the Security Test effort.
- Ensure that the proper personnel are involved in the Security Test, and coordinate schedule changes.
- Review the Security Test report.

4.3. Other Supporting Organizations or Working Groups

Other HUD organizations external to the ST&E team may be called upon to support [System Name] certification testing. This support is specified in the Security Test Plan.

5.0 Plans of Actions and Milestones

Plans of Actions and Milestones (POA&M) document corrective actions resulting from an ST&E. A POA&M serves as a tool to develop, implement, and manage corrective action plans for a system. The POA&M for the [System Name] is found within the Certification Package.[1]

The contents of the POA&M columns are as described below:

- **ID** – Provides a cross reference number to facilitate tracking of corrective actions.
- **Weaknesses** – Describes the weakness identified during the ST&E.
- **POC** – Identifies the office or organization that the agency head will hold responsible for resolving the weakness.
- **Resources Required –** Estimates funding resources required to resolve the weakness.
- **Scheduled Completion Date** – Provides the scheduled completion date for resolving the weakness.
- **Milestones with Completion Dates** – Documents key milestones with completion dates.
- **Milestone Changes** – Identifies milestone changes as the POA&M is updated.
- **Identified in Chief Financial Officer (CFO) Audit or other review?** – Identifies the source (e.g. program review, Inspector General (IG) audit, General Accounting Office (GAO) audit, etc.) of the weakness.
- **Status** – Provides the status of the corrective action.
- **Risk Ranking –** Provides level of risk affecting the evaluated information system.

Weaknesses and corrective action will be listed in the POA&M according to risk, with those posing the highest degree of risk listed first.

[1] HUD uses the POA&M format required for reporting weaknesses to OMB. This format was derived from OMB Memorandum 02-09.

DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

SECURITY TEST AND EVALUATION (ST&E) RESULTS REPORT TEMPLATE
Version 1.0

April 2005

[SYSTEM NAME]
[Organization]

[DATE PREPARED]

Prepared by:

Preparing Organization

6.0 Security Test & Evaluation Results

The Security Test & Evaluation was conducted on System Name in accordance with the Security Test & Evaluation Plan dated MM/DD/YY. Testing was accomplished in the following fashion:

- Date (Start Time to End Time): Analyst Name assisted by Name of System Representative tested Category of Controls Tested (i.e., Management, Operational, or Technical)

- Date (Start Time to End Time): Analyst Name assisted by Name of System Representative tested Category of Controls Tested (i.e., Management, Operational, or Technical)

- Date (Start Time to End Time): Analyst Name assisted by Name of System Representative tested Category of Controls Tested (i.e., Management, Operational, or Technical)

The results of all security testing are tabulated in the Security Test Result Report (Table 6-1). Testing requirements were defined by using NIST SP 800-53 as the minimum security requirements, and augmenting these minimum security requirements based on the system criticality and sensitivity as noted in the risk assessment report. The minimal security requirements and testing procedures were augmented to include industry best practices regarding system specific and vender specific security controls.

- Security controls relating to, hardware, software, operating system, applications, and databases on the system (technology-driven).
- Security controls based on the increased levels of concern for confidentiality, integrity, and availability (sensitivity-driven).
- Security controls based on the internal or external exposure and risk based decisions (exposure/risk-driven).

The results of testing the minimum security requirements are provided in the Security Test Results Report (Table 6-1). Security test procedures in Appendix A supply system specific findings related to Test Result report (Table 6-1).

The following figures summarize findings documented in Table 6-1:

[Insert Total System Controls and associated text and name it “Figure 1”]

[Insert Management Controls Summary and associated text and name it “Figure 2”]

[Insert Operational Controls Summary and associated text and name it “Figure 3”]

[Insert Technical Controls Summary and associated text and name it “Figure 4”]

TABLE 6-1. SECURITY TEST RESULTS REPORT

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
Management Class						
RA	**Risk Assessment**	**Is risk assessed?**				
RA-1	**Risk Assessment Policy and procedures**	Are risks to organizational operations and assets resulting from the operation of the information system identified?	Verify by inspection. Review risk assessment policies. Review most recent high-level risk assessment. (FISCAM SP-1)			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
RA-2	**Security Categorization**	Has data sensitivity and integrity of the data been considered?	Verify by reviewing appropriate document. Risk Assessment and/or Threat Analysis documents may exist separately or be included in Security Plan, but should contain security categorization.			The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations
RA-3	**Risk Assessment**	Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change?	Verify by inspection. Review recent risk assessment. Verify risk assessment is conducted on a regular basis or on other conditional change.			The organization conducts 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.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
RA-4	**Risk Assessment Update**	Are risks to organizational operations and assets updated and do they reflect operation of the information system identified?	The Risk Assessment dated MM/DD/YYYY identifies possible threat sources and methods of mitigation.			The organization updates the risk assessment every three years 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**	Are systems periodically reviewed for known vulnerabilities and software patches promptly installed?	Obtain recent vulnerability scan conducted by organization.			Vulnerability Scanning: Using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information system every six months or when significant new vulnerabilities affecting the system are identified and reported.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
RA-5.1	**Vulnerability Scanning**	Do vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned?				Vulnerability scanning tools include the capability to readily update the list of vulnerabilities scanned.
RA-5.2	**Vulnerability Scanning**	Does the organization update the list of information system vulnerabilities every six months or when significant new vulnerabilities are identified and reported?				Vulnerability Scanning: The organization updates the list of information system vulnerabilities every six months or when significant new vulnerabilities are identified and reported.
RA-5.3	**Vulnerability Scanning**	Vulnerability scanning procedures include means to ensure adequate scan coverage, both vulnerabilities checked and information system components scanned.				**This Control is Not Required for High Level Systems**

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
PL	**Planning**	**Is security planning conducted?**				
PL-1	**Security Planning Policy and Procedures**	Is there a security planning policy and procedure developed that is consistent with applicable federal laws, directives, policies, regulations, standards, and guidance?	Review security planning policies and procedures, ensure that policies and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

SYSTEM NAME Security Test & Evaluation

		System Classification Level	3	**High**		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
PL-2	**System Security Plan**	Has a system security plan been developed that provides an overview of the security requirements for the system with a description of the security controls in place or planned?	Review system security plan.			The organization develops and implements 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 review and approve the plan.
PL-3	**System Security Plan Update**	Does the organization review the security plan for the information and revise the plan to address system organizational changes or problems identified during plan implementation or security controls assessments?	Verify by inspection			The organization reviews the security plan for the information system [Assignment: organization-defined frequency] and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments.
PL-4	**Rules of Behavior**	Has Rules of Behavior been established, disseminated, and signed by all users of the system? The ROB should describe user responsibilities and expected behavior with regard to information system usage.	Review Rules of Behavior and verify content.			The organization establishes and makes readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information system usage. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PL-5	**Privacy Impact Assessment**	Has the organization conducted a privacy impact assessment on the information system?	Verify by inspection. Review most recent high level security plan for inclusion of privacy impact analysis.			The organization conducts a privacy impact assessment on the information system.
SA	**System and Services Acquisition**	**Are system and services acquisitions addressed?**				
SA-1	**System Services Acquisition Policy and Procedures**	Are there established information system policies and procedures for acquisition of system services?	Review Systems Services Policy			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and services acquisition policy that addresses purpose, scope, roles, responsibilities, 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.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
SA-2	**Allocation of Resources**	Does the organization determine, document and allocate resources as a part of the capital planning and investment control process to ensure any investment request includes the security resources needed?	Verify by inspection that security resources for the system have been justified in the capital planning process.			The organization determines, documents, and allocates as part of its capital planning and investment control process the resources required to adequately protect the information system.
SA-3	**Life Cycle Support**	Is the information system development life cycle clearly defined?	Review System Life Cycle Development Documentation.			The organization manages the information system using a system development life cycle methodology that includes information security considerations.
SA-4	**Acquisitions**	Does the organization include security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk?	Review security requirements.			The organization includes security requirements and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
SA-5	**Information System Documentation**	In accordance with organizational policy, are there detailed procedures developed, documented, and effectively implemented to ensure that adequate documentation is available for the information system?	Review system documentation i.e. user manuals. Vendor supplied documentation, in house application manuals and hardware and software testing results.			The organization ensures that adequate documentation for the information system and its constituent components is available, protected when required, and distributed to authorized personnel.
SA-5.1	**Information System Documentation**	Is there sufficient documentation that describes the functional properties of the security controls?	Verify by inspection			The organization includes documentation describing the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
SA-5.2	**Information System Documentation**	Is there sufficient documentation that describes the design and implementations details for the security controls employed within the system?	Verify by inspection			The organization includes documentation describing the design and implementation details of the security controls employed within the information system with sufficient detail to permit analysis and testing of the controls (including functional interfaces among control components).
SA-6	**Software Usage Restriction**	Is the use of copyrighted software or shareware and personally owned software/equipment documented in accordance with organization's software usage restrictions?	Review Security policy			The organization complies with software usage restrictions.
SA-7	**User Installed Software**	Does the organization enforce explicit rules governing the downloading and installation of software by users?	Review Security Plan and rules of behavior.			The organization enforces explicit rules governing the downloading and installation of software by users.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
SA-8	**Security Design Principles**	In accordance with organizational policy, does the organization design and implement the information system using security engineering principles?	Review Development documentation.			The organization designs and implements the information system using security engineering principles.
SA-9	**Outsourced Information System Services**	In accordance with organizational policy, are there detailed procedures developed, documented, and effectively implemented to reduce risks from outsourced services by explicitly addressing the need for effective security controls at the service provider?	Review Service Provider (3rd party/outsourced service) and Contractor Security Plans and procedures to verify reduction of risk of introducing a security flaw or breach to the organization			The organization ensures that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements. The organization monitors security control compliance.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
SA-10	**Developers Configuration Management**	Does the system developer create and implement configuration management plans that control changes to system during development?	Review System Development documentation and Configuration management plan.			The information system developer creates and implements a configuration management plan that controls changes to the system during development, tracks security flaws, requires authorization of changes, and provides documentation of the plan and its implementation.
SA-11	**Developers Security Testing**	Does the information system developer create a security test and evaluation plan, implement the plan, and document the results?	Review Testing Plans and Testing controls and standards used during security testing.			The information system developer creates a security test and evaluation plan, implements the plan, and documents the results. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.
CA	**Certification, Accreditation**	**Are Certification and Accreditation activities**				

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
CA-1	**Certification, Accreditation, and Security Assessment Policies and Procedures**	Does the system comply with formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls?	Verify through inspection and demonstration. Review most recent certification documents. Review procedures.			The organization develops, disseminates, and periodically reviews/updates: (i) formal, documented, security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, 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**	Does the organization conduct an assessment of the security controls in the information system 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?	Verify through inspection and demonstration. Review procedures.			The organization conducts an assessment of the security controls in the information system 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.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
CA-3	**Information System Connections**	Does the organization authorize all connections from the information system to other information systems outside of the accreditation boundary and monitor/control the system interconnections on an ongoing basis? Do appropriate organizational officials approve information system interconnection agreements?	Verify that interconnections are authorized by examining MOUs or other documentation.			The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary and monitors/controls the system interconnections on an ongoing basis. Appropriate organizational officials approve information system interconnection agreements.
CA-4	**Security Certification**	Does the organization 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?	Verify that policy, procedure, and documentation exists. Verify that system configuration shows that controls are implemented.			The organization conducts 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.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
CA-5	**Plan of Action and Milestones**	Does the organization develop and update quarterly a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system?	Verify through inspection that POA&M exists and cover all required areas.			The organization develops and updates quarterly, a plan of action and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.
CA-6	**Security Accreditation**	Does the organization authorize (i.e., accredit) the information system for processing before operations and updates the authorization every three years? Does a senior organizational official sign and approve the security accreditation?	Verify through inspection that system has been accredited for processing, and that accreditation is updated every three years, and signed by a senior organizational official.			The organization authorizes (i.e., accredits) the information system for processing before operations and updates the authorization every 3 years. A senior organizational official signs and approves the security accreditation.
CA-7	**Continuous Monitoring**	Does the organization monitor the security controls in the information system on an ongoing basis?	Verify through inspection of the change management and system documentation. (FISCAM SS-3.1, 3.2 AND CC-2.1)			The organization monitors the security controls in the information system on an ongoing basis.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
Operational Class						
PS	**Personnel Security**	**Is personnel security addressed?**				
PS-1	**Personnel Security Policy and Procedures**	Does the system owner comply with organizational policy by formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls?	Verify by inspection of policy and procedures.			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PS-2	**Position Categorization**	Does the organization assign a risk designation to all positions and establishes screening criteria for individuals filling those positions? Does the organization review and revise position risk designations [Assignment: organization-defined frequency]?	Verify by inspection of risk designation and screening criteria. Inspect, review and revise documentation.			The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations [Assignment: organization-defined frequency].
PS-3	**Personnel Screening**	Does the organization screen individuals requiring access to organizational information and information systems before authorizing access?	Verify by inspection of screening documentation.			The organization screens individuals requiring access to organizational information and information systems before authorizing access.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PS-4	**Personnel Termination**	When employment is terminated, does the organization terminate information system access, conduct exit interviews, ensure the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensure that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems?	Verify by inspection of documentation.			When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.
PS-5	**Personnel Transfer**	Does the organization review information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiate appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations)?	Verify by inspection of documentation.			The organization reviews information systems/facilities access authorizations when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorizations).

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
PS-6	**Access Agreements**	Does the organization complete appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access?	Verify by inspection of documentation.			The organization completes appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access.
PS-7	**Third-Party Personnel Security**	Does the organization established personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitor provider compliance to ensure adequate security?	Verify by inspection of documentation.			The organization establishes personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitors provider compliance to ensure adequate security.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	**3**	**High**		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
PS-8	**Personnel Sanctions**	Does the organization employ a formal sanctions process for personnel failing to comply with established information security policies and procedures?	Verify by inspection of documentation.			The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.
PE	**Physical and Environmental Protection**	**Is physical and environmental protection addressed?**				
PE-1	**Physical and Environmental Protection Policy and Procedures**	Does the organization develop, disseminate, and periodically review/update: (i) a formal, documented, Physical security policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls?	Review policy and procedures			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, 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.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PE-2	**Physical Access Authorizations**	Does the organization develops and maintain a current list of personnel with authorized access to facilities containing information system?				The organization develops and keeps current lists of personnel with authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials once a year.
PE-3	**Physical Access Control**	Does the organization control all physical access points to facilities containing information systems?				The organization controls all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities. The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PE-4	**Access Control for Transmission Medium**	Is physical access to data transmission lines controlled?	Verify by observation			**This Control is Not Required for High Level Systems**
PE-5	**Access Control for Display Medium**	Are computer monitors located to eliminate viewing by unauthorized persons?	Verify by observation			The organization controls physical access to information system devices that display information to prevent unauthorized individuals from observing the display output.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PE-6	**Monitoring Physical Access**	Does the organization monitor physical access to information system to detect and respond to incidents?				The organization monitors physical access to information systems to detect and respond to incidents.
PE-6.1	**Monitoring Physical Access**	Does the organization monitors real-time intrusion alarms and surveillance equipment?	Verify by inspection			The organization monitors real-time intrusion alarms and surveillance equipment.
PE-6.2	**Monitoring Physical Access**	Does the organization employ automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated?	Verify by inspection			The organization employs automated mechanisms to ensure potential intrusions are recognized and appropriate response actions initiated.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PE-7	**Visitor Control**	Does the organization control physical access to information system by authenticating visitors before authorizing access to sensitive areas?				The organization controls physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible.
PE-7.1	**Visitor Control**	Is visitor control addressed?	Verify by inspection			The organization escorts visitors and monitors visitor activity, when required.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PE-8	**Access Logs**	Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken?	Check Risk Assessment and Security Plan for identification of sensitive facilities in compliance with NIST 800-60			The organization maintains a visitor access log to facilities (except for those areas within the facilities 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 review the access logs [Assignment: organization-defined frequency] after closeout.
PE-8.1	**Access Logs**	Does the organization employ automated mechanisms to facilitate the maintenance and review of access logs?	Check physical access control list for sensitive areas and facilities			The organization employs automated mechanisms to facilitate the maintenance and review of access logs.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PE-9	**Power Equipment and Power Cabling**	Does the organization protect power equipment and power cabling for the information system?	Verify by inspection			The organization protects power equipment and power cabling for the information system from damage and destruction.
PE-10	**Emergency Shutoff**	Does the organization provide the capability of shutting off power to any information technology component?	Check audit logs and review audit log procedures for monitoring of physical access to sensitive areas			For specific locations within a facility containing concentrations of information system resources (e.g., data centers, server rooms, mainframe rooms), the organization provides the capability of shutting off power to any information technology component that may be malfunctioning (e.g., due to an electrical fire) or threatened (e.g., due to a water leak) without endangering personnel by requiring them to approach the equipmen
PE-11	**Emergency Power**	Does the organization provide short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event loss of primary power source?	Verify by observation and check physical access audit logs for preplanned appointments and visitor handling			The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PE-12	**Emergency Lighting**	Does the organization employ and maintain automatic emergency lighting systems?				The organization employs and maintains automatic emergency lighting systems that activate in the event of a power outage or disruption and that cover emergency exits and evacuation routes.
PE-13	**Fire Protection**	Does the organization employ and maintain fire suppression and detection devices/systems that can be manually or automatically activated in the even of a fire?				The organization employs and maintains fire suppression and detection devices/systems that can be activated in the event of a fire..
PE-13.1	**Fire Protection**	Is fire protection addressed?				Fire suppression and detection devices/systems activate automatically in the event of a fire.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PE-13.2	**Fire Protection**	Do fire suppression and detection devices/systems provide automatic notification of any activation to the organization and emergency responders?				Fire suppression and detection devices/systems provide automatic notification of any activation to the organization and emergency responders.
PE-14	**Temperature and Humidity Controls**	Does the organization regularly maintain and monitor the temperature and humidity within facilities containing information systems?	Verify physical access controls by observation			The organization regularly maintains within acceptable levels and monitors the temperature and humidity within facilities containing information systems.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PE-15	**Water Damage Protection**	Does the organization protect the information system from water damage resulting from damaged plumbing lines or other sources of water leakages?				The organization protects the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shutoff valves are accessible, working properly, and known to key personnel.
PE-15.1	**Water Damage Protection**	Does the organization employ automated mechanisms to automatically close shutoff valves in the event of a significant water leak?				The organization employs automated mechanisms to automatically close shutoff valves in the event of a significant water leak.
PE-16	**Delivery and Removal**	Does the organization control and inventory hardware, software and information technology media entering and exiting the facility?	Review Disaster Recovery Plan and associated documents for plans to reduce the potential damage from plumbing leaks			The organization controls information system-related items (i.e., hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
PE-17	**Alternate Work Site**	Does the organization employ appropriate information security controls at the alternate work site?	Review Building Safety Plan and Disaster Recovery Plan for the provision of emergency lighting			Individuals within the organization employ appropriate information system security controls at alternate work sites.
CP	**Contingency Planning and Operations**	Is contingency planning addressed?				

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
CP-1	**Contingency Planning Policy and Procedures**	Does the system owner comply with formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls?	Verify contingency plan through inspection to assure that it covers all required areas. Review documented procedures on implementation.			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
CP-2	**Contingency Plan**	Does the organization 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? Do designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel?	Verify through inspection to assure that contingency plan covers all required areas. Review documented procedures on implementation.			The organization develops and implements 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 review and approve the contingency plan and distribute copies of the plan to key contingency personnel.
CP-2 .1	**Contingency Plan**	Does the organization coordinate contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan)?	Verify through inspection that contingency plan is coordinated with all other related plans.			The organization coordinates contingency plan development with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).
CP-3	**Contingency Training**	Does the organization train personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training at least annually?	Verify through inspection that training records are kept.			The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training annually.

SYSTEM NAME Security Test & Evaluation

		System Classification Level	3	**High**		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
CP-3 .1	**Contingency Training**	Does the organization incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations?	Verify through inspection of documentation that contingency training contains simulated events.			The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.
CP-3 .2	**Contingency Training**	Does the organization employ automated mechanisms to provide a more thorough and realistic training environment?	Verify by observation.			**This Control is Not Required for High Level Systems**
CP-4	**Contingency Plan Testing**	Does the organization test the contingency plan for the information system at least annually to determine the plan's effectiveness and the organization's readiness to execute the plan? Are systems rated as high tested at the alternate processing site? Do appropriate officials within the organization review the contingency plan test results and initiate corrective actions?	Verify by inspection that records are kept on annual testing, testing of high systems at alternate site, and that appropriate officials take appropriate action.			The organization tests the contingency plan for the information system at least annually using to determine the plan's effectiveness and the organization's readiness to execute the plan. System rated as high shall be tested at the alternate processing site. Appropriate officials within the organization review the contingency plan test results and initiate corrective actions.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
CP-4 .1	**Contingency Plan Testing**	Does the organization coordinate contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan)?	Verify through inspection that contingency plan testing is coordinated with all other related plans.			The organization coordinates contingency plan testing with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan).
CP-4 .2	**Contingency Plan Testing**	Does the organization test the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations?	Verify through inspection of documentation that contingency training is performed at alternate site.			The organization tests the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.
CP-4 .3	**Contingency Plan Testing**	Does the organization employ automated mechanisms to more thoroughly and effectively test the contingency plan?	Verify through inspection of automated mechanisms.			**This Control is Not Required for High Level Systems**

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
CP-5	**Contingency Plan Update**	Does the organization review the contingency plan for the information system once per year and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing?	Verify through inspection of documentation.			The organization reviews the contingency plan for the information system once per year and revises the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing.
CP-6	**Alternate Storage Sites**	Does the organization identify an alternate storage site and initiate necessary agreements to permit the storage of information system backup information?	Verify through review of documentation.			The organization identifies an alternate storage site and initiates necessary agreements to permit the storage of information system backup information. The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.
CP-6 .1	**Alternate Storage Sites**	Is the alternate storage site geographically separated from the primary storage site so as not to be susceptible to the same hazards?	Verify through review of documentation.			The alternate storage site is geographically separated from the primary storage site so as not to be susceptible to the same hazards.
CP-6 .2	**Alternate Storage Sites**	Is the alternate storage site configured to facilitate timely and effective recovery operations?	Verify through review of documentation.			The alternate storage site is configured to facilitate timely and effective recovery operations.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
CP-6 .3	**Alternate Storage Sites**	Does the organization identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions?	Verify through review of documentation.			The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
CP-7	**Alternate Processing Sites**	Does the organization identify an alternate processing site and initiate necessary agreements to permit the resumption of information system operations for critical mission/business functions within 24 hours when the primary processing capabilities are unavailable?	Verify through inspection of agreements such as MOUs and SLAs and also contingency plan documentation.			The organization identifies an alternate processing site and initiates necessary agreements to permit the resumption of information system operations for critical mission/business functions within 24 hours when the primary processing capabilities are unavailable.
CP-7 .1	**Alternate Processing Sites**	Is the alternate processing site geographically separated from the primary processing site so as not to be susceptible to the same hazards?	Verify that this is identified in contingency plan.			The alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
CP-7 .2	**Alternate Processing Sites**	Does the organization identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions?	Verify that this is identified in contingency plan.			The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
CP-7 .3	**Alternate Processing Sites**	Do alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements?	Verify through inspection of agreements such as MOUs and SLAs.			Alternate processing site agreements contain priority-of-service provisions in accordance with the organization's availability requirements.
CP-7 .4	**Alternate Processing Sites**	Is the alternate processing site fully configured to support a minimum required operational capability and is it ready to use as the operational site?	Verify that this is identified in contingency plan.			The alternate processing site is fully configured to support a minimum required operational capability and ready to use as the operational site.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
CP-8	**Telecommunications Services**	Does the organization identify primary and alternate telecommunications services to support the information system and initiate necessary agreements to permit the resumption of system operations for critical mission/business functions within 24 hours when the primary telecommunications capabilities are unavailable?	Verify through inspection of service agreements.			The organization identifies primary and alternate telecommunications services to support the information system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions within 24 hours when the primary telecommunications capabilities are unavailable.
CP-8 .1	**Telecommunications Services**	Do primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements?	Verify through inspection of service agreements.			Primary and alternate telecommunications service agreements contain priority-of-service provisions in accordance with the organization's availability requirements.
CP-8 .2	**Telecommunications Services**	Are alternate telecommunications services configured to not share a single point of failure with primary telecommunications services?	Verify through inspection of telecommunications documentation.			Alternate telecommunications services do not share a single point of failure with primary telecommunications services.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
CP-8.3	**Telecommunications Services**	Are alternate telecommunications service providers sufficiently separated from primary service providers so as not to be susceptible to the same hazards?	Verify through inspection of telecommunications documentation.			Alternate telecommunications service providers are sufficiently separated from primary service providers so as not to be susceptible to the same hazards.
CP-8 .4	**Telecommunications Services**	Do primary and alternate telecommunications service providers have adequate contingency plans?	Verify through inspection of telecommunications documentation.			Primary and alternate telecommunications service providers have adequate contingency plans.
CP-9	**Information System Backup**	Does the organization conduct backups of user-level and system-level information (including system state information) contained in the information system according to backup schedules documented in the system contingency plan, and store backup information at an appropriately secured location?	Verify through inspection that configuration policy and settings are configured for backups as appropriate.			The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and stores backup information at an appropriately secured location.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
CP-9 .1	**Information System Backup**	Does the organization test backup information to ensure media reliability and information integrity?	Examine the backup storage site and backup schedule documentation.			The organization conducts backups of user-level and system-level information (including system state information) contained in the information system according to backup schedules documented in the system contingency plan and stores backup information at an appropriately secured location.
CP-9 .2	**Information System Backup**	Does the organization selectively use backup information in the restoration of information system functions as part of contingency plan testing?	Verify through inspection of testing documentation.			The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.
CP-9 .3	**Information System Backup**	Does the organization store backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software?	Verify through inspection of contingency plan.			The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.
CP-10	**Information System Recovery and Reconstitution**	Does the organization employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure?	Verify through inspection of mechanisms.			The organization employs mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
CP-10.1	**Information System Recovery and Reconstitution**	Does the organization include a full recovery and reconstitution of the information system as part of contingency plan testing?	Verify through inspection of contingency plan.			The organization includes a full recovery and reconstitution of the information system as part of contingency plan testing.
CM	**Configuration Management**	**Is configuration management addressed?**				
CM-1	**Configuration Management Plan**	Has the organization developed, disseminated, reviewed and updated policies and procedures for configuration management that are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance?	Review organizational policies and procedures for configuration management. Ensure that policies and procedures have been developed, disseminated, reviewed, and updated. The policies and procedures should be consistent with applicable federal laws, directives, policies,			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
			regulations, standards, and guidance.			
CM-2	**Baseline Configuration**	Has the organization developed, documented, and maintained a current baseline configuration of the information system and inventory of the system's constituent components?	Review configuration management documentation to ensure that a baseline configuration has been documented and is current.			The organization develops, documents, and maintains a current, baseline configuration of the information system and an inventory of the system's constituent components.
CM-2 .1	**Baseline Configuration**	Does the organization update baseline configurations as an integral part of information system component installations?	Review configuration management documentation to ensure that a baseline configuration has been documented and is current.			The organization updates the baseline configuration as an integral part of information system component installations. Plan includes explicit checks with assigned responsibilities to periodically ensure that the plan is being implemented as intended.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
CM-2 .2	**Baseline Configuration**	Does the organization employ automated mechanisms to maintain up-to-date, complete, accurate, and readily available baseline configuration?	Verify by interview and inspection the use of automated mechanisms to maintain baseline configurations. Review baseline configuration output from the automated mechanism and test the baseline against a organizational information system.			The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration.
CM-3	**Configuration Change Control**	Does the organization document and control changes to the information system? Has the organization developed emergency change procedures and added the procedures to the configuration management process? Has the appropriate organizational officials approved changes to information system with respect to organizational policies and procedures?	Review change control documentation to review documented changes to the system and who approved the change. Ensure that emergency change procedures have been documented and added to configuration management process.			The organization documents and controls changes to the information system. Appropriate organizational officials approve information system changes in accordance with organizational policies and procedures.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
CM-3.1	**Configuration Change Control**	Has the organization employed automated mechanisms to document changes, notify appropriate approving officials, highlight approvals that have not been received in a timely manner, controls changes to system until necessary approvals are received and documents completed changes to the system?	Review output from automated mechanism to ensure that changes are documented, appropriate approving officials have been notified, changes that aren't responded to in a prompt manner are highlighted. Ensure that the information system controls/inhibits changes to the system until the necessary approval has been provided.			The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.
CM-4	**Monitoring Configuration Changes**	Does the organization monitor changes to the information system and conduct security impact analysis to determine effects of the changes?	Verify by Inspection that the organization monitors changes to the system. Verify procedures and test results from security impact analysis on existing security controls.			The organization monitors changes to the information system and conducts security impact analyses to determine the effects of the changes.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
CM-5	**Access Restriction For Change**	Does the organization enforce access restrictions associated with changes to the information system?	Verify by interview and inspection that access restrictions are in place when changes are made to the system. Ensure that administrators are the only individuals that can make changes to the system.			The organization enforces access restrictions associated with changes to the information system.
CM-5 .1	**Access Restriction For Change**	Does the organization employ automated mechanisms to enforce access restrictions and support auditing of the enforcement actions?	Verify by inspection and interview that automated mechanisms are used to enforce access restriction and actions are audited.			The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.
CM-6	**Configuration Settings**	Does the organization configure the security settings of the information technology products to the most restrictive mode that is consistent with the operational needs of the information system?	Verify by inspection that security settings are set to the most restrictive mode.			The organization configures the security settings of information technology products to the most restrictive mode consistent with information system operational requirements.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
CM-6.1	**Configuration Settings**	Does the organization employ automated mechanisms to centrally manage, apply, and verify configuration settings?	Verify by interview and inspection. Review output and configuration of the automated mechanism.			The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.
CM-7	**Least Functionality**	Does the organization configure the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of ports, protocols, and services.	The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of any protocol or service that is not explicitly permitted			The organization configures the information system to provide only essential capabilities and specifically prohibits and/or restricts the use of any protocol or service that is not explicitly permitted.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
CM-7.1	**Least Functionality**	Does the organization review information systems to identify and eliminate unnecessary functions, ports, protocols, and services?	The organization reviews the information system annually, to identify and eliminate unnecessary functions, ports, protocols, and/or services			The organization reviews the information system annually, to identify and eliminate unnecessary functions, ports, protocols, and/or services.
MA	**Maintenance**	Is maintenance addressed?				

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
MA-1	**System Maintenance Policy and Procedures**	Has the organization developed, disseminated, periodically review, and update a information system policy and procedure that address purpose, scope, roles, responsibilities, and compliance for performing maintenance on a information system?	Review by inspection organizational maintenance policies and procedures to ensure they are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.
MA-2	**Periodic Maintenance**	Does the organization schedule, perform, and document routine preventive/regular maintenance to the components of the information system?	Review by inspection; maintenance documentation and logs to verify schedule and ensure regular maintenance of information system components.			The organization schedules, performs, and documents routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
MA-2 .1	**Periodic Maintenance**	Does the organization maintain a maintenance log for the information system, that includes, date, time, name of person performing maintenance, name of individual that escorted maintenance personnel, description and a list of equipment removed or added to the information system?	Review maintenance logs for content.			The organization maintains a maintenance log for the information system that includes: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).
MA-2.2	**Periodic Maintenance**	Has the organization employed automated mechanisms to ensure periodic maintenance is scheduled and conducted as required. Ensure that maintenance log contains actions, both needed and completed, and is up-to-date?	Review by interview inspection. Review output from automated system of scheduled maintenance and actions performed during maintenance of the information system. Ensure that log is compete and up-to-date.			The organization employs automated mechanisms to ensure that periodic maintenance is scheduled and conducted as required, and that a log of maintenance actions, both needed and completed, is up to date, accurate, complete, and available.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
MA-3	**Maintenance Tools**	Does the organization approve, control, and monitor the use of information system maintenance tools and maintain the tools on an ongoing basis.	Verify by interview and inspection. The organization document approvals and monitor use of maintenance tools.			The organization approves, controls, and monitors the use of information system maintenance tools and maintains the tools on an ongoing basis.
MA-3 .1	**Maintenance Tools**	Does the organization inspect all maintenance tools carried into the facility by maintenance personnel for obvious improper modifications?	Verify by inspection, documented log of tools and configured settings. The organization inspects all maintenance tools that enter the facility.			The organization inspects all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
MA-3 .2	**Maintenance Tools**	Does the organization check all media containing diagnostic test programs for malicious code before the media is used in the information system?	Verify by inspection, documented log of media containing diagnostic test programs. The organization checks all media containing diagnostic programs for malicious code before the media can be used on the information system.			The organization checks all media containing diagnostic test programs (e.g., software or firmware used for system maintenance or diagnostics) for malicious code before the media are used in the information system.
MA-3 .3	**Maintenance Tools**	Does the organization check all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is properly sanitized. If the equipment is not sanitized, it will remain with the facility or be destroyed?	Verify by inspection; documented log of maintenance equipment. Verify log of equipment that is left with the facility and/or destroyed. Ensure organization has proper equipment for sanitizing media.			The organization checks all maintenance equipment with the capability of retaining information to ensure that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; if the equipment cannot be sanitized, the equipment remains within the facility or is destroyed, unless an appropriate organization official explicitly authorizes an exception.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
MA-3 .4	**Maintenance Tools**	Does the organization employ automated mechanisms to ensure only authorized personnel use maintenance tools?	Verify by inspection list of authorized personnel that can use maintenance tools.			**This Control is Not Required for High Level Systems**
MA-4	**Remote Maintenance**	Does the organization approve, control, and monitor remotely executed maintenance and diagnostic activities?	Verify by inspection and interview approval documentation for remote access to perform maintenance. Ensure that restrictions are in place on who performs maintenance and verify audit trail (monitoring) of actions.			The organization approves, controls, and monitors remotely executed maintenance and diagnostic activities.
MA-4.1	**Remote Maintenance**	Does the organization audit all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions?	Verify by interview and inspection; the existence of audit information of remote access for maintenance and who reviews the logs.			The organization audits all remote maintenance sessions, and appropriate organizational personnel review the audit logs of the remote sessions.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
MA-4.2	**Remote Maintenance**	Does the organization address the installation and use of remote diagnostic links in the security plan for the information system?	Review Security plan to verify that the organization addresses the installation and use of remote diagnostic links.			The organization addresses the installation and use of remote diagnostic links in the security plan for the information system.
MA-4.3	**Remote Maintenance**	If remote diagnostic or maintenance services are performed, does the service or organization performing them implements for its own information system the same level of security as that implemented on the information system being serviced?	Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced.			Remote diagnostic or maintenance services are acceptable if performed by a service or organization that implements for its own information system the same level of security as that implemented on the information system being serviced.
MA-5	**Maintenance Personnel**	Does the organization maintain a list of personnel authorized to perform maintenance on the information system?	Verify by inspection the list of authorized personnel that can perform maintenance actions on the system.			The organization maintains a list of personnel authorized to perform maintenance on the information system. Only authorized personnel perform maintenance on the information system.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
MA-6	**Timely Maintenance**	Does the organization obtain maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure?	The organization obtains maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure			The organization obtains maintenance support and spare parts for [Assignment: organization-defined list of key information system components] within [Assignment: organization-defined time period] of failure.
	System and Communication Protection	Is system and communication protection addressed?				
SI-1	**System and Information Integrity Policy and Procedures**	In accordance with organizational policy, are there detailed system and information integrity procedures developed, documented, and effectively implemented?	Review System and Information integrity policy. Review Security Plan.			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and information integrity policy that addresses purpose, scope, roles, responsibilities, 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.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
SI-2	**Flaw Remediation**	Does the organization identify, report and correct information system flaws?	Review reports.			The organization identifies, reports, and corrects information system flaws.
SI-3	**Malicious Code Protection**	Does the information system implement malicious code protection that includes a capability for automated updates?	Verify by inspection			The information system implements malicious code protection that includes a capability for automatic updates.
SI-3 .1	**Malicious Code Protection**	Does the organization centrally manage virus protection mechanisms?	Review virus scanning software configuration. Interview appropriate personnel.			The organization centrally manages virus protection mechanisms.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
SI-3 .2	**Malicious Code Protection**	Does the information system automatically update virus protection mechanisms?	Verify by inspection			The information system automatically updates virus protection mechanisms.
SI-4	**Intrusion Detection Tools and Techniques**	Does the organization employ tool and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system?	Verify by inspection			The organization employs 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**	Does the organization receive information system security alerts/advisories on a regular basis, issue alerts/advisories to appropriate personnel, and take appropriate actions in response?	Verify by inspection			The organization receives information system security alerts/advisories on a regular basis, issues alerts/advisories to appropriate personnel, and takes appropriate actions in response.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
SI-6	**Security Functionality Verification**	Does the information system verify the correct operation of security functions periodically every year and notify system administrator when anomalies are discovered?	Verify by inspection and interview.			The information system verifies the correct operation of security functions periodically every year and notifies system administrator when anomalies are discovered.
SI-6 .1	**Security Functionality Verification**	Does the organization employ automated mechanisms to provide notification of failed security tests?	Verify by inspection and interview.			The organization employs automated mechanisms to provide notification of failed security tests.
SI-7	**Software and Information Integrity**	Does the information system detect and protect against unauthorized changes to software and information?	Verify by inspection.			The information system detects and protects against unauthorized changes to software and information.
SI-8	**Spam and Spyware Protection**	Does the information system implement spam and spyware protection?	Verify by inspection.			The information system implements spam and spyware protection.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
SI-8.1	**Spam and Spyware Protection**	Does the organization centrally manage spam and spyware protection mechanisms?	Verify by inspection.			The organization centrally manages spam and spyware protection mechanisms.
SI-9	**Information Input Restriction**	Does the organization restrict the information input to the system to authorized personnel only?	Verify by inspection.			The organization restricts the information input to the information system to authorized personnel only.
SI-10	**Information Input Accuracy, Completeness, and Validity**	Does the information system check information inputs for accuracy completeness and validity?				The information system checks information inputs for accuracy, completeness, and validity.
SI-11	**Error Handling**	Does the information system identify and handle error conditions in a timely manner?	Verify by inspection.			The information system identifies and handles error conditions in an expeditious manner.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
SI-12	**Information Output Handling and Retention**	Does the organization handle and retain output from the information system in accordance with organization policy and operational requirements?	Review security plan for periodic security awareness training for security personnel			The organization handles and retains output from the information system in accordance with organizational policy and operational requiements.
MP	**Media Protection**	Are media protection policies and procedures documented and implemented correctly?				

SYSTEM NAME Security Test & Evaluation

		System Classification Level	3	**High**		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
MP-1	**Media Protection Policy and Procedures**	Does the organization develop, disseminate, and periodically review/update: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls?	Verify by inspection of documentation.			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, 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**	Does the organization ensure that only authorized users have access to information in printed form or on digital media removed from the information system?	Verify by inspection of documentation.			The organization ensures that only authorized users have access to information in printed form or on digital media removed from the information system.
MP-2 .1	**Media Access**	Unless guard stations control access to media storage areas, does the organization employ automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted?	Inspect automated mechanisms and associated documentation.			Unless guard stations control access to media storage areas, the organization employs automated mechanisms to ensure only authorized access to such storage areas and to audit access attempts and access granted.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
MP-3	**Media Labeling**	Does the organization affix external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information?	Verify by inspection of removable storage media and system output.			The organization affixes external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information.
MP-4	**Media Storage**	Does the organization physically control and securely store information system media, both paper and electronic, based on the highest FIPS 199 security category of the information recorded on the media?	Verify by inspection of information storage.			The organization physically controls and securely stores information system media, both paper and electronic, based on the highest FIPS 199 security category of the information recorded on the media.
MP-5	**Media Transport**	Does the organization control information system media (paper and electronic) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel?	Verify by inspection of documentation.			The organization controls information system media (paper and electronic) and restricts the pickup, receipt, transfer, and delivery of such media to authorized personnel.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
MP-6	**Media Sanitization**	Does the organization sanitize information system digital media using approved equipment, techniques, and procedures? Does the organization track, document, and verify media sanitization actions, and periodically test sanitization equipment/procedures to ensure correct performance?	Verify by inspection of documentation.			The organization sanitizes information system digital media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization actions and periodically tests sanitization equipment/procedures to ensure correct performance.
MP-7	**Media Destruction and Disposal**	Does the organization sanitize or destroy information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media?	Verify by inspection of documentation.			The organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media.
IR	**Incident Response**	Are incident response policies and procedures documented and implemented effectively?				

SYSTEM NAME Security Test & Evaluation

		System Classification Level	3	**High**		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
IR-1	**Incident Response policy and Procedures**	Has the organization developed, disseminated, periodically reviewed, and updated a formal policy and procedure for incident response?	Review organizational policies and procedures for incident response.			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, 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**	Does the organization train personnel in their incident response roles and responsibilities with respect to the information system and provide refresher training?	The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training at least annually. Verify documented evidence that training of organizational personnel takes place to include the roles and responsibilities of the personnel in training.			The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training at least annually.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
IR-2.1	**Incident Response Training**	Does the organization incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations?	Verify by inspection simulated incident response events that take place.			The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.
IR-2.2	**Incident Response Training**	Does the organization employ automated mechanisms to provide a more thorough and realistic training environment?	Verify by inspection the use of automated mechanisms and the material provided.			The organization employs automated mechanisms to provide a more thorough and realistic training environment.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
IR-3	**Incident Response Testing**	Does the organization test the incident response capability for the information system at least annually using organization defined test and exercises to determine the incident response effectiveness and documents the results?	The organization tests the incident response capability for the information system at least annually using automated mechanisms for high systems to determine the incident response effectiveness and documents the results			The organization tests the incident response capability for the information system at least annually using automated mechanisms for high systems to determine the incident response effectiveness and documents the results.
IR-3.1	**Incident Response Testing**	Does the organization employ automated mechanisms to more thoroughly and effectively test the incident response capability?	Verify by inspection use of automated mechanisms, the input and output from testing the incident response capability.			The organization employs automated mechanisms to more thoroughly and effectively test the incident response capability.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
IR-4	**Incident Handling**	Has the organization implemented an incident handling capability for security incidents to include preparation, detection, and analysis, containment, eradication, and recovery?	Verify incident handling procedures of security incidents.			The organization employs automated mechanisms to support the incident handling process.
IR-4.1	**Incident Handling**	Does the organization employ automated mechanisms to support the incident handling process?	Verify by inspection the use of automated mechanisms. Verify configuration of system and output provided to help in incident response capability.			The organization employs automated mechanisms to support the incident handling process.
IR-5	**Incident Monitoring**	Does the organization track and document information system security incidents on an ongoing basis?	Verify documented log of information system security incidents.			The organization tracks and documents information system security incidents on an ongoing basis.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
IR-5.1	**Incident Monitoring**	Does the organization employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information?	Verify by inspection the use of automated mechanisms and review output.			The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.
IR-6	**Incident Reporting**	Does the organization promptly report incident information to appropriate authorities?	Verify by inspection; Incident report and who the report was provided to.			The organization promptly reports incident information to appropriate authorities.
IR-6	**Incident Reporting**	Does the organization employ automated mechanisms to assist in the reporting of security incidents?	Verify by inspection the use of automated mechanisms and output (report) of security incident.			The organization employs automated mechanisms to assist in the reporting of security incidents.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
IR-7	**Incident Response Assistance**	Does the organization have a help desk group that offers advice and assistance to users of the information system for the handling and reporting of security incidents?	A help desk or group that offers advice is available for support and security needs.			The organization provides an incident 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.
IR-7.1	**Incident Response Assistance**	Does the organization employ automated mechanisms to increase the availability of incident response-related information and support.	Verify by inspection and interview the use of automated mechanisms and review output.			The organization employs automated mechanisms to increase the availability of incident response-related information and support.
AT	**Awareness and Training**	Are awareness and training activities performed?				

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
AT-1	**Security Awareness and Training Policy and Procedures**	Does the organization develop, disseminate, and periodically review/update: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, 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?	Verify through inspection by obtaining handouts and follow directions to access security procedures and policies			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, 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**	Does the organization ensure that all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and at least annually thereafter?				The organization ensures all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to the system and at least annually thereafter.
AT-3	**Security Training**	Does the organization identify personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system and	Verify by inspection and interview.			The organization identifies personnel with significant information system security roles and responsibilities, documents those roles and responsibilities, and provides appropriate information system security training before authorizing access to the system and each year thereafter.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
		each year thereafter?				
AT-4	**Security Training Records**	Does the organization document and monitor individual information system security training activities including basic security awareness training and specific information system security training?	Verify by inspection and interview.			The organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.
TECHNICAL CLASS						

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
	Identification and Authentication	Is identification and authentication addressed?				
IA-1	**Individual Identification and Authentication Policy and Procedures**	Does the organization develop, disseminate, periodically review, and update and formal policy and procedure for identification and authentication?	Verify organizations policy and procedure for identification and authentication.			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, 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**	Does the information system uniquely identify and authenticate users?	Passwords are unique and difficult to guess (e.g., such as requiring alpha/numeric, upper/lower case, and special characters.			The information system uniquely identifies and authenticates users (or processes acting on behalf of users).

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
IA-2 .1	**User Identification and Authentication**	Does the information system employ multifactor authentication?	Verify by inspection. The information system employs multifactor authentication.			The information system employs multifactor authentication.
IA-3	**Device Identification and Authentication**	Does the information system identify and authenticate specific devices before establishing a connection?	The information system identifies and authenticates specific devices before establishing a connection.			The information system identifies and authenticates specific devices before establishing a connection.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
IA-4	**Identifier Management**	Does the organization manage user identifiers?	Verify by inspection of documentation and interview system administrator. The organization manages user identifiers by uniquely identifying each user, verifying the identity of each user, receiving authorization to issue a user identifier, and ensuring that identifier is handed to the appropriate intended party.			The organization manages user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling user identifier after [Assignment: organization-defined time period] of inactivity; and (vi) archiving user identifiers.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
IA-5	**Authentication Management**	Does the organization manage information system authenticators?	Verify by inspection and interview. The organization manages information system authenticators by defining initial authenticator content, establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators, and changing default authenticators upon information system installation.			The organization manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon information system installation.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
IA-6	**Authentication Feedback**	Does the information system provide feedback to a user during an attempted authentication and is feedback configured so as not to compromise the authentication mechanism?	Verify by inspection; attempt to log into the system, using valid and invalid means of authentication. The information system provides feedback to a user during an attempted authentication and the feedback does not compromise the authentication mechanism.			The information system provides feedback to a user during an attempted authentication and that feedback does not compromise the authentication mechanism.
IA-7	**Cryptographic Module Authentication**	Does the information system employ authentication methods that meet the requirements of FIPS 140-2 when authenticating to a cryptographic module?	Verify by interview and inspection that authentication methods to cryptographic modules meet federal standards.			For authentication to a cryptographic module, the information system employs authentication methods that meet the requirements of FIPS 140-2.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
AC	**Access Control**	Is access control addressed?				
AC-1	**Access Control Policy and Procedures**	Has the system owner formally documented procedures to facilitate the implemented organization access control policy?	Review system access control policy			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
AC-2	**Account Management**	Does the organization manage and review information system account?	Review System account procedures.			The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [Assignment: organization-defined frequency].

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
AC-2 .1	**Account Management**	In accordance with organizational policy, are there automated mechanisms in place and detailed supporting procedures are developed, documented, and effectively implemented to provide access protections for remote connections?	Review security plan for mechanisms that verify the sending or receipt of messages. Review sample configurations.			The organization employs automated mechanisms to support the management of information system accounts.
AC-2 .2	**Account Management**	Do the organization terminate temporary and emergency accounts after 48 hours?	Review policy and procedures			The information system automatically terminates temporary and emergency accounts after 48 hours.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
AC-2 .3	**Account Management**	Does the organization terminate inactive accounts after a specific period of time?	Review policy and procedures			The information system automatically disables inactive accounts after 90 Days.
AC-2 .4	**Account Management**	Are there automated mechanisms in place and detailed supporting procedures developed, documented, and effectively implemented to enable user-commanded locking of the information system session?	Review sample configurations.			The organization employs automated mechanisms to ensure that account creation, modification, disabling, and termination actions are audited and, as required, appropriate individuals are notified.
AC-3	**Access Enforcement**	Are there automated mechanisms in place and detailed supporting procedures developed, documented, and effectively implemented to enable enforcement of defined actions in the event of session inactivity?	Review sample configurations.			The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy.

SYSTEM NAME Security Test & Evaluation

System Classification Level	3	**High**

ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
AC-3.1	**Access Enforcement**	Does the information system enforce assigned authroizations for controlling access to the system in accordance with applicable policy?	Review security plan for limitations on object reuse. Review system configurations for memory and partitioning.			The information system ensures that access to security functions (deployed in hardware, software, and firmware) and information is restricted to authorized personnel (e.g., security administrators).
AC-4	**Information Flow enforcement**	Does the information system enforce assigned authorization for controlling the flow of information within the system between interconnected systems?	Review mechanism configurations. Review Configuration policy.			The information system enforces 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**	Does the organization and information system enforce the separation of duties through assigned access authorizations?	Review job assignments. Review configuration.			The information system enforces separation of duties through assigned access authorizations.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
AC-6	**Least Privilege**	Does the configuration policy and information systems setting enforce the most restrictive set of rights/ privileges or accesses needed by users to perform their specified tasks?	Review Configuration policy. Review sample device configurations.			The information system enforces 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**	Does the configuration policy and information system setting enforce a limit of three consecutive invalid access attempts by a user during a 30 minute time period?	Review Configuration policy. Review sample device configurations.			The information system enforces a limit of three consecutive invalid access attempts by a user during a 30 minute time period. The information system automatically locks the account/node for 30 minutes for low systems or until an appropriate security administrator manually intervenes to unlocks accounts on moderate and high systems when the maximum number of unsuccessful attempts is exceeded.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
AC-8	**System Use Notification**	Does the configuration policy and information system settings display an approved, system use notification message?	Review Configuration policy. Review sample device configurations.			The information system displays 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 provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.
AC-9	**Previous Logon Notifications**	Is the configuration policy and information system settings configured to notify the user upon successful logon, date and time of last logon, and the number of unsuccessful logon attempts since last successful logon?	Review Configuration policy. Review sample device configurations.			**This Control is Not Required for High Level Systems**

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
AC-10	**Concurrent Session Control**	Are the system configuration policy and information system device settings configured to restrict concurrent sessions?	Review Configuration policy. Review sample device configurations.			The information system does not allow concurrent sessions for systems rated high.
AC-11	**Session Lock**	Are the configuration policy and information system settings configured to prevent further access to the system by initiating a session lock that remains in effect until the authorized user reestablishes access?	Review Configuration policy. Review sample device configurations.			The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
AC-12	**Session Termination**	Are the configuration policy and information system settings configured to automatically terminate a session after ten minutes of inactivity?	Review configuration policy. Review configurations.			The information system automatically terminates a session after ten minutes of inactivity.
AC-13	**Supervision and Review - Access Control**	Does the organization superviseand review the activities of users to enforce usage of information system access controls?	Review Configuration audit policy. Review auditing configurations.			The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls.
AC-13.1	**Supervision and Review - Access Control**	Does the organization employ automated mechanisms to facilitate the review of user activities?	Review Configuration policy. Review configurations.			The organization employs automated mechanisms to facilitate the review of user activities.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
AC-14	**Permitted Actions Without identification or Authentication**	Does the organization identify specific users action that can be performed on the information system without identification or authentication?	Review configuration policy.			The organization identifies specific user actions that can be performed on the information system without identification or authentication.
AC-14.1	**Permitted Actions Without identification or Authentication**	Does the organization permit actions that can be performed on the information system without identification or authentication?				The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.

SYSTEM NAME Security Test & Evaluation

		System Classification Level	**3**	**High**		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
AC-15	**Automated Marking**	Does the organization and information system utilize standard naming conventions to identify any special dissemination, handling, or distribution instructions?				The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions.
AC-16	**Automated Labeling**	Does the organization and information system utilize appropriate labels in storage, in process and in transmission?	Verify by inspection			**This Control is Not Required for High Level Systems**
AC-17	**Remote Access**	Does the organization document, monitor, and control all methods of remote access to the information system?	Review Organization policy. Review configuration.			The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, Internet) to the information system including remote access for privileged functions. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.
AC-17.1	**Remote Access**	Does the organization employ automated mechanisms to facilitate monitoring and control of remote access methods?	Review Organization policy. Review configuration. Verify by inspection			The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

SYSTEM NAME Security Test & Evaluation

System Classification Level	3	**High**

ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
AC-17.2	**Remote Access**	Does the organization employ encryption to protect the confidentiality of the remote access session?	Review Organization policy. Review configuration. Verify by inspection			The organization uses encryption to protect the confidentiality of remote access sessions.
AC-17.3	**Remote Access**	Does the organization control all remote accesses through a managed access control point?	Review Organization policy. Review configuration. Verify by inspection			The organization controls all remote accesses through a managed access control point.
AC-18	**Wireless Access Restrictions**	Does the organization document, (including restrictions) monitor, and control all methods of wireless access to the information system?	Review wireless policy.			The organization: (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.
AC-18.1	**Wireless Access Restrictions**	Does the organization employ encryption to protect the wireless access to the information system?	Review Organization policy. Review configuration. Verify by inspection			The organization uses authentication and encryption to protect wireless access to the information system.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
AC-19	**Access Control for Portable and Mobile Devices**	Does the organization document, (including restrictions) monitor, and control the use of portable and mobile devices that access to the information system?	Review policy and procedures			The organization: (i) establishes usage restrictions and implementation guidance for portable and mobile devices; and (ii) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.
AC-19.1	**Access Control for Portable and Mobile Devices**	Does the organization employ removable hard drives or cryptography to protect information residing or portable and mobile devices?	Review policy and procedures. Verify by inspection.			The organization employs removable hard drives or cryptography to protect information residing on portable and mobile devices.
AC-20	**Personally owned Information Systems**	Does the organization restrict the use personally owned information systems?	Review policy and procedures.			The organization restricts the use of personally owned information systems for official U.S. Government business involving the processing, storage, or transmission of federal information.
AU	**Audit and Accountability**	**Is audit and accountability addressed?**				

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
AU-1	**Audit and Accountability Policy and Procedures**	Does the organization develop, disseminate, and periodically review/update: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls?	Verify through inspection of policy and procedures.			The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, 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**	Does the information system generate audit records for the following events: [Assignment: organization-defined auditable events]?	Verify through inspection of logs and history reports.			The information system generates audit records for the following events: [Assignment: organization-defined auditable events].

SYSTEM NAME Security Test & Evaluation

		System Classification Level	3	**High**		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
AU-2.1	**Auditable Events**	Does the information system provide the capability to compile audit records from multiple components throughout the system into a system wide (logical or physical), time-correlated audit trail?	Verify through inspection and demonstration. Review procedures.			**This Control is Not Required for High Level Systems**
AU-2.2	**Auditable Events**	Does the information system provide the capability to manage the selection of events to be audited by individual components of the system?	Verify through inspection and demonstration. Review procedures.			**This Control is Not Required for High Level Systems**
AU-3	**Content of Audit Records**	Does the information system capture sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events?	Verify through inspection of logs and history reports.			The information system captures sufficient information in audit records to establish what events occurred, the sources of the events, and the outcomes of the events.
AU-3.1	**Content of Audit Records**	Does the information system provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject?	Verify through inspection and demonstration. Review procedures.			The information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject.

SYSTEM NAME Security Test & Evaluation

		System Classification Level	3	**High**		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
AU-3.2	**Content of Audit Records**	Does the information system provide the capability to centrally manage the content of audit records generated by individual components throughout the system?	Verify through inspection and demonstration. Review procedures.			The information system provides the capability to centrally manage the content of audit records generated by individual components throughout the system.
AU-4	**Audit Storage Capacity**	Does the organization allocate sufficient audit record storage capacity and configure auditing to prevent such capacity being exceeded?	Verify through inspection and demonstration. Review procedures.			The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded.
AU-5	**Audit Processing**	In the event of an audit failure or audit storage capacity being reached, does the information system alert appropriate organizational officials and take the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shutdown information system, overwrite oldest audit records, stop generating audit records)].	Verify through inspection and demonstration. Review procedures.			In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shutdown information system, overwrite oldest audit records, stop generating audit records)].
AU-5.1	**Audit Processing**	Does the information system provide a warning when allocated audit record storage volume is close to being reached?	Verify through inspection and demonstration. Review procedures.			The information system provides a warning when allocated audit record storage volume is close to being reached.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
AU-6	**Audit Monitoring, Analysis, and Reporting**	Does the organization regularly review/analyze audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions?	Verify through inspection and demonstration. Review procedures.			The organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions.
AU-6.1	**Audit Monitoring, Analysis, and Reporting**	Does the organization employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities?	Verify through inspection and demonstration. Review procedures.			The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.
AU-6.2	**Audit Monitoring, Analysis, and Reporting**	Does the organization employ automated mechanisms to immediately alert security personnel of inappropriate or unusual activities with security implications?	Verify through inspection and demonstration. Review procedures.			**This Control is Not Required for High Level Systems**
AU-7	**Audit Reduction and Report Generation**	Does the information system provide an audit reduction and report generation capability?	Verify through inspection and demonstration. Review procedures.			The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
AU-7.1	**Audit Reduction and Report Generation**	Does the information system provide the capability to automatically process audit records for events of interest based upon selectable, event criteria?	Verify through inspection and demonstration. Review procedures.			The information system provides the capability to automatically process audit records for events of interest based upon selectable, event criteria.
AU-8	**Time Stamps**	Does the information system provides time stamps for use in audit record generation?	Verify through inspection and demonstration.			The information system provides time stamps for use in audit record generation.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
AU-9	**Protection of Audit Information**	Does the information system protect audit information and audit tools from unauthorized access, modification, and deletion?	Verify through inspection and demonstration. Review procedures.			The information system protects audit information and audit tools from unauthorized access, modification, and deletion.
AU-9.1	**Protection of Audit Information**	Does the information system produce audit information on hardware-enforced, write-once media?	Verify through inspection and demonstration. Review procedures.			**This Control is Not Required for High Level Systems**

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
AU-10	**None Repudiation**	Does the information system provide the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message)?	Verify through inspection and demonstration. Review procedures.			**This Control is Not Required for High Level Systems**
AU-11	**Audit Retention**	Does the organization retain audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements?	Verify through inspection and demonstration. Review procedures.			The organization retains audit logs in accordance with HUD records retention policies, but at least for one year for high and moderate systems to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
SC	**System and Communication Protection**	Is system and communication protection addressed?				

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
SC-1	**System and Communication Protection Policy and Procedures**	Does the system owner ensure that procedures comply with formal document organization policy to facilitate the implementation of the system communication protection policy?				The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, 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**	Are the configuration policy and information system settings configured to enforce separation of user functionality from information system management functionality?	Verify by inspection			The information system separates user functionality (including user interface services) from information system management functionality.
SC-3	**Security Function Isolation**	Does the configuration policy and system configuration settings isolate security functions from non security functions?	Review configuration policy. Verify by inspection.			The information system isolates security functions from nonsecurity functions.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
SC-4	**Information Remnants**	Does the configuration policy and system configuration settings prevent unauthorized and unintended information transfer via shared system resources?	Review configuration policy. Verify by inspection.			The information system prevents unauthorized and unintended information transfer via shared system resources.
SC-5	**Denial of Service Protection**	Does the configuration policy and system configuration settings protect against or limit the effect of denial of service attacks on devices within the organization's internal network?	Review Configuration policy. Verify by inspection.			The information system protects against or limits the effects of denial of service attacks on devices within the organization’s internal network.
SC-6	**Resource Priority**	Does the information system limit the use of resources by priority?	Review Configuration policy. Verify by inspection.			The information system limits the use of resources by priority.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	**SECURITY CONTROLS NAME**	**SECURITY CONTROL**	**ST&E ACTIONS**	**800-53 Status**	**Pass / Fail**	**EXPECTED RESULTS**
SC-7	**Boundary Protection**	Does the information system monitor and control communication at the external boundary of the information system and at key internal boundaries within the system?	Review Configuration policy. Verify by inspection.			The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system.
SC-7.1	**Boundary Protection**	Does the organization physically allocate publicly accessible information system components to separate sub networks and separate, physical network interfaces?	Review Configuration policy. Verify by inspection.			The organization physically allocates publicly accessible information system components (e.g., public web servers) to separate subnetworks with separate, physical network interfaces. The organization prevents public access into the organization's internal networks except as appropriately mediated.
SC-8	**Transmission Integrity**	Does the configuration policy protect the integrity of transmitted information?	Review Configuration policy. Verify by inspection.			The information system protects the integrity of transmitted information.

SYSTEM NAME Security Test & Evaluation

System Classification Level	3	**High**

ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
SC-8.1	**Transmission Integrity**	Does the organization employ cryptographic mechanisms?	Review Configuration policy. Verify by inspection.			The organization employs cryptographic mechanisms to ensure recognition of changes to information during transmission unless otherwise protected by alternative physical measures (e.g., protective distribution systems).
SC-9	**Transmission Confidentiality**	Does the information system protect the confidentiality of transmitted information?	Review Configuration policy. Verify by inspection.			The information system protects the confidentiality of transmitted information
SC-9.1	**Transmission Confidentiality**	Does the organization employ cryptographic mechanisms to prevent unauthorized disclosure of information during transmission?	Verify by inspection			The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless protected by alternative physical measures (e.g., protective distribution systems).

SYSTEM NAME Security Test & Evaluation

System Classification Level	3	**High**

ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
SC-10	**Network Disconnect**	Does the information system terminate a network connection at the end of a session or after ten minutes of inactivity?	Review Configuration policy. Verify by inspection.			The information system terminates a network connection at the end of a session or after ten minutes of inactivity.
SC-11	**Trusted Path**	Has the information system established a trusted communication path between the user and the security functionality of the system?				**This Control is Not Required for High Level Systems**
SC-12	**Cryptographic Key Establishment and Management**	Does the information system employ automated mechanisms for cryptographic key establishment and key management?	Review Configuration policy and procedures. Verify by inspection.			The information system employs automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management.
SC-13	**Use of Validation Cryptography**	If encryption is used, does it meet federal standards?				When cryptography is employed within the information system, the system performs all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
SC-14	**Public Access Protections**	Does the information system protect the integrity of the publicly available information system and applications?	Review Configuration policy and procedures. Verify by inspection.			For publicly available systems, the information system protects the integrity of the information and applications.
SC-15	**Collaborative Computing**	Does the information system prohibit remote activation of collaborative computing mechanisms?				The information system prohibits remote activation of collaborative computing mechanisms (e.g., video and audio conferencing) and provides an explicit indication of use to the local users (e.g., use of camera or microphone).
SC-16	**Transmission of Security Parameters**	Are internal security labels (naming conventions) used to control access to specific information types or files?	Verify by inspection.			**This Control is Not Required for High Level Systems**
SC-17	**Public Key Infrastructure Certificates**	Has the organization developed and implemented a certification policy and certification procedure statement for the issuance of public key certificates used in the information system?	Verify by inspection.			The organization develops and implements a certificate policy and certification practice statement for the issuance of public key certificates used in the information system.

SYSTEM NAME Security Test & Evaluation						
		System Classification Level	3	High		
ID	SECURITY CONTROLS NAME	SECURITY CONTROL	ST&E ACTIONS	800-53 Status	Pass / Fail	EXPECTED RESULTS
SC-18	**Mobile Code**	Is the used of mobile code documented and monitored within the information system?	Review security policy.			The organization: (i) establishes 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) documents, monitors, and controls the use of mobile code within the information system. Appropriate organizational officials authorize the use of mobile code.
SC-19	**Voice Over Internet Protocol**	Has the organization established usage restrictions and implementation guidance for Voice Over Internet Protocol (VOIP) technologies?	Review VOIP policy and implementation guidance.			The organization: (i) establishes 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) documents, monitors, and controls the use of VOIP within the information system. Appropriate organizational officials authorize the use of VOIP.

Appendix A - Test Procedures

Appendix A maps special test procedures to requirements in Table 6.1

Test Number:	SITE:	DATE:
Test Name: Windows NT/2000		
Resources Required**:**	Primary Domain Controllers (PDC) for all network domains to be tested and for any workstations that are also to be tested.	
Personnel Required:	Network Administrators with Domain Administrator privileges for the network to be tested, and a Network Security Administrator.	
Objectives:	To determine if the network domain controllers and workstations are configured correctly and securely.	
Procedure Description: (Summary)	Review system settings on the domain controllers and selected workstations. Interview Network Administrators and Network Security Administrators.	

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
1.	10.2.6	Are all hard drives formatted to a secure file system?	Hard drives are formatted to a secure file system.		
2.	10.3.2	Are Service Packs identified and tracked for each server?	Service Packs are tracked and identified for each server.		
3.	15.1.12	Are logons cached on security sensitive servers?	Logons are not cached on security sensitive servers.		
4.	10.1.4	Is system boot time set to zero seconds?	System boot time is set to zero seconds.		
5.	15.1.7	What is the minimum password length allowed?	The minimum password length is appropriate for the system being reviewed.		
6.	15.1.7	Is password complexity enabled?	Password complexity is enabled. All passwords are required to be alphanumeric.		
7.	15.1.6	How frequently are administrative passwords changed?	Administrative passwords are changed at least every 60 days.		
8.	11.2.3	How many previous passwords are remembered by the system?	Password history is set to at least 4 passwords.		
9.	15.1.14	How many unsuccessful login attempts are required to	A maximum of three unsuccessful login attempts locks out an		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
		lock out an account? How is the account re-enabled?	account. An Administrator is required to re-enable the account.		
10.	17.1.1	Are the Security Access Matrix (SAM) database/Shadow Password files encrypted using strong encryption?	The SAM database/Shadow Password files are encrypted using strong encryption.		
11.	17.1.6	Is auditing enabled at the operating system level? If so, what is being audited?	Auditing is enabled at the operating system level. All appropriate events for the platform are being audited.		
12.	17.1.4	How long are the audit logs archived?	Audit logs are archived for a minimum of one year.		
13.	9.2.7	Are all samples, examples, and application documentation removed from the servers?	All samples, examples, and application documentation are removed from the servers.		
14.	6.1.3	Who has the ability to add, change, or remove system or application level files?	Only system administrators have the ability to add, change, or remove system or application level files.		
15.	11.1	Which systems have anti-virus software installed on them?	All computers have anti-virus software installed on them.		
16.	11.1.2	How is the anti-virus software configured?	The anti-virus software is configured to scan all files accessed on that computer.		
17.	11.1.1	How frequently is the anti-virus software updated? Who reviews the update logs? When are they reviewed?	The anti-virus software is updated regularly. The updated logs are reviewed weekly by a manager responsible for the network.		
18.	4.1.1	Are change control/ configuration management procedures followed for all software and hardware modifications of systems that process and store sensitive information?	Change control/configuration management procedures are followed for all software and hardware modifications to systems that process and store sensitive information.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
19.	15.1.8	How long after a console session becomes idle, does the system automatically lock out? Does the system require a password to reactivate the session?	The system automatically locks out a console session after 15 minutes of inactivity. A password is required to reactivate the session.		
20.	10.3.2	Are security patches tested to ensure the expected level of protection is provided?	Security patches are tested to ensure that the expected level of protection is provided.		
21.	16.1.3	Are the appropriate Access Control Lists (ACLs) set for system files, administrative tools, system registry entries, and files that control security services in applications?	The appropriate ACLs are set for system files, administrative tools, system registry entries, and files that control security services in applications.		
22.	16.1.6	Is the NTFS “eight-dot-three” name generation turned off?	The NTFS 8.3 name generation ability is turned off.		
23.	16.1.3	Are the appropriate ACLs set for the default Windows repair directory?	The appropriate ACLs are set for the default Windows repair directory.		
24.	16.1.3	Are the OS/2 and POSIX subsystems removed if they are not used?	The OS/2 and POSIX subsystems are removed if they are not used.		
25.	16.1.3	Are unnecessary Net and Administrative Shares removed?	Unnecessary Net and Administrative Shares are removed.		
26.	16.2.2	Has TCP/IP filtering been configured for each network card using the TCP/IP protocol?	TCP/IP filtering has been configured for each network card that is using the TCP/IP protocol.		
27.	16.1.3	Have unused ODBC/OLE-DB database drivers and unnecessary Component Object Module (COM) components been removed?	Unused ODBC/OLE-DB database drivers and unnecessary COM components have been removed.		
28.	15.1.9	Is the last logon user name hidden from the	The last logon user name is hidden from the		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
		next system user?	next system user.		
29.	16.2.13	Is a legal notice displayed on the screen that warns authorized and unauthorized users that the system is being monitored to detect improper use of the system and other illicit activities, that there is no expectation of privacy on the system, and that defines what is considered proper use of the system before a user logs on?	A legal notice is displayed on the screen that warns authorized and unauthorized users that the system is being monitored to detect improper use of the system and other illicit activities, that there is no expectation of privacy on the system, and that defines what is considered proper use of the system before a user logs on.		
30.	16.2.12	Is the guest account renamed and disabled?	The guest account is renamed and disabled.		
31.	10.2.6	Has the original Administrator account been renamed, moved to the Guest Group, and configured to allow only a network lockout for this account?	The original Administrator account has been renamed, moved to the Guest Group, and configured to allow only a network lockout for this account.		
32.	16.2.5	Has anonymous network and registry access been restricted?	Anonymous network and registry access has been restricted.		
33.	16.2.5	Is unauthenticated remote access to the registry prevented?	Unauthenticated remote access to the registry is prevented.		
34.	16.2.3	Is static routing used on sensitive and mission critical systems?	Static routing is used on sensitive and mission critical systems.		

Test Number:	SITE:	DATE:
Test Name: Sun Solaris		
Resources Required**:**	All servers and related workstations using the Sun Solaris operating system.	
Personnel Required:	System Administrators with administrator privileges to the systems to be tested, and a System Security Administrator.	
Objectives:	To determine if the Solaris systems are configured correctly and securely.	
Procedure Description:(Summary)	Review system settings on the Solaris systems. Interview System Administrators and System Security Administrators.	

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
1.	11.2.3	Verify that the security mode has been changed and a password set in the OpenBoot PROM.	The security mode has been changed and a password set in the OpenBoot PROM.		
2.	16.2.3	Verify that an Authorized Use banner is used (OEM-banner and interactive session banners) and that all banners are the same.	An Authorized Use banner is used (OEM-banner and interactive session banners) and all banners are the same.		
3.	16.2.3	Verify that the interactive banner files have file access permissions set to 444, are owned by *root*, and group ownership is set to *sys* or *bin*.	The interactive banner files have file access permissions set to 444, are owned by *root*, and group ownership is set to *sys* or *bin*.		
4.	16.2.3	Verify that warning banners are deployed on all display devices allowing application or command-level access and that banners state (at a minimum): accessing the system constitutes consent to system monitoring for law enforcement and other purposes and unauthorized users of the system may be subject to criminal prosecution and/or criminal or civil	Banners state the necessary information and comply with the minimum standard.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
		penalties.			
5.	10.3.2	Verify that tracking and identification of system patches occurs.	Tracking and identification of system patches occurs.		
6.	15.1.7	Verify that user passwords comply with existing written policy or existing Federal standards, whichever is more restrictive, and that password complexity is enforced.	Passwords comply with the requisite standard and password complexity has been implemented.		
7.	15.1.6	Verify that administrative passwords are changed bi-monthly.	Administrative passwords are changed bi-monthly.		
8.	11.2.3	Verify that new passwords must be different from the previous four.	New passwords must be different from the previous four.		
9.	15.1.14	Verify that repeated unsuccessful attempts (maximum of three) to access an account (login) results in an account lock out and requires a System Administrator to re-enable.	Repeated unsuccessful attempts results in an account lock out and require a System Administrator to re-enable.		
10.	11.2.3	Verify that systems protect passwords via either a shadow password file or the passwd.adjunct file.	Systems protect passwords using either a shadow password file or a passwd.adjunct file.		
11.	16.2.3	Verify that users requiring root privileges log on to their personal account and invoke the su - command to switch *user* to *root*.	Users requiring root privileges log on to their personal account and invoke the su - command to switch *user* to *root*.		
12.	16.2.3	Verify that all privileged user's personal PATH statements are bound by the same restrictions as the *root* PATH statement.	All privileged user's personal PATH statements are bound by the same restrictions as the *root* PATH statement.		
13.	16.2.3	Verify that *root* only logs on from the system console.	*Root* only logs on from the system console.		
14.	17.1.1	Verify that when	When administrators log		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
		administrators log on as *root* from the system console, they record the event by making an entry in the system logbook that records date, time, and actions performed and why.	on as *root* from the system console, they record the event by making an entry in the system logbook that records date, time, and actions performed and why.		
15.	11.2.3	Verify that all systems that are accessed remotely using the *root* password, or any other privileged account password, use Secure Shell (ssh), or an equivalent, to accomplish I&A with encryption.	All systems that are accessed remotely using the *root* password, or any other privileged account password, use Secure Shell (ssh), or an equivalent, to accomplish I&A with encryption.		
16.	17.1.1	Verify that when ssh is used the capability to log on directly as *root* is disabled.	When ssh is used the capability to log on directly as *root* is disabled.		
17.	10.1.2	Verify that only privileged users and groups have access to kernel capabilities.	Only privileged users and groups have access to kernel capabilities.		
18.	1.2.3	Verify that every account is assigned to at least one group.	Every account is assigned to at least one group.		
19.	1.2.3	Verify that a file integrity system is used to monitor changes to sensitive system files.	A file integrity system is used to monitor changes to sensitive system files.		
20.	1.2.3	Verify that world writeable files are only allowed in public directories, such as /tmp, /var/tmp, etc.	World writeable files are only allowed in public directories, such as /tmp, /var/tmp, etc.		
21.	1.2.3	Verify that world writeable directories are only allowed if they are public directories, such as /tmp, /var/tmp, or other documented directories, and that they have the sticky bit set.	World writeable directories are only allowed if they are public directories, such as /tmp, /var/tmp, or other documented directories, and they have the sticky bit set.		
22.	1.2.3	Ensure that all daemons have permissions of 755, or	All daemons have permissions of 755, or more restrictive.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
		more restrictive.			
23.	1.2.3	Ensure that all system log files have permissions of 744, or more restrictive.	All system log files have permissions of 744, or more restrictive.		
24.	1.2.3	Ensure that all default/skeleton dot files have permissions of 744, or more restrictive.	All default/skeleton dot files have permissions of 744, or more restrictive.		
25.	1.2.3	Ensure that all shells have permissions of 755, or more restrictive.	All shells have permissions of 755, or more restrictive.		
26.	1.2.3	Verify that all system commands have permissions of 755, or more restrictive.	All system commands have permissions of 755, or more restrictive.		
27.	1.2.3	Verify that all system files, programs, and directories are owned by a privileged account (i.e., an account with a uid less than 21) and belong to a privileged group (i.e., gid less than 20).	All system files, programs, and directories are owned by a privileged account (i.e., an account with a uid less than 21) and belong to a privileged group (i.e., gid less than 20).		
28.	11.2.3	Verify that *root* owns the password and password shadow files (or equivalent).	*Root* owns the password and password shadow files (or equivalent).		
29.	1.2.3	Verify that shadow files, or the equivalent, are readable and writeable only by root or the system default owner.	Shadow files, or the equivalent, are readable and writeable only by root or the system default owner.		
30.	11.2.3	Ensure that the /etc/passwd file has permissions of 644, or more restrictive.	The /etc/passwd file has permissions of 644, or more restrictive.		
31.	11.2.3	Verify that the /etc/shadow file has permissions of 400.	The /etc/shadow file has permissions of 400.		
32.	1.2.3	Ensure that each user is assigned a home directory in the /etc/passwd file.	Each user is assigned a home directory in the /etc/passwd file.		
33.	11.2.3	Verify that home directories defined in the /etc/passwd file exist.	A sampling of home directories defined in the /etc/passwd file does exist.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
34.	1.2.3	Verify that home directories have an initial access permission of 700 and that they are not allowed to be more permissive than 750.	A sampling of home directories shows them to have an initial access permission of 700 and that they are not more permissive than 750.		
35.	1.2.3	Verify that the *user* or *root* owns the user startup files.	A sampling of user startup files shows that the *user* or *root* owns those files.		
36.	1.2.3	Verify that user startup files have permissions of 740, or more restrictive.	A sampling of user startup files shows that the files have permissions of 740, or more restrictive.		
37.	1.2.3	Verify that user startup files do not have a "." or a "::" in the PATH variable definition except as the last entry.	A sampling of user startup files shows that the files do not have a "." or a "::" in the PATH variable definition except as the last entry.		
38.	1.2.3	Verify that user and system startup files do not have the *suid* bit set.	A sampling of user startup files shows that the files do not have the *suid* bit set.		
39.	1.2.3	Verify that user and system startup files do not have the *sgid* bit set.	A sampling of user startup files shows that the files do not have the *sgid* bit set.		
40.	1.2.3	Verify that user startup files do not contain the command *mesg -y*.	A sampling of user startup files shows that the files do not contain the command *mesg -y*.		
41.	1.2.3	Verify that system startup files are owned by root.	The system startup files are owned by root.		
42.	1.2.3	Verify that the system startup files have a group owner of bin, sys, or the system default.	The system startup files have a group owner of bin, sys, or the system default.		
43.	1.2.3	Verify that access permissions for system startup files (except symbolic links which should be 777) are 755, or more restrictive.	Access permissions for system startup files are 755 or more restrictive. Access permissions for symbolic links are 777.		
44.	1.2.3	Verify that system startup files do not contain ".", "::" (or a ":"	System startup files do not contain ".", "::" (or a ":" as the last entry) in		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
		as the last entry) in the PATH variable.	the PATH variable.		
45.	1.2.3	Verify that system startup files contain the command *mesg -n*.	System startup files contain the command *mesg -n*.		
46.	1.2.3	Verify that all shells are owned by *root* or *bin*.	All shells are owned by *root* or *bin*.		
47.	1.2.3	Verify that shells have access permissions of 755 or more restrictive.	Shells have access permissions of 755 or more restrictive.		
48.	1.2.3	Verify that the console device (i.e., /dev/console) is not world readable or world writeable.	The console device (i.e., /dev/console) is not world readable or world writeable.		
49.	9.1.1	Verify that backup device (tape and floppy disk device) files are not world writeable unless justified and documented with the ISSO/SA.	Backup device (tape and floppy disk device) files are not world writeable unless justified and documented with the ISSO/SA.		
50.	1.2.3	Verify that user file systems, removable media, or remote file systems are not mounted with the *nosuid* option invoked.	User file systems, removable media, or remote file systems are not mounted with the *nosuid* option invoked.		
51.	1.2.3	Verify that the sticky bit is set on all public directories.	The sticky bit is set on all public directories.		
52.	1.2.3	Verify that the owner of public directories (directories with the sticky bit set) is *root*.	The owner of public directories (directories with the sticky bit set) is *root*.		
53.	1.2.3	Verify that the group owner of all public directories is *root*, *sys*, *bin*, or the COTS/GOTS default.	The group owner of all public directories is *root*, *sys*, *bin*, or the COTS/GOTS default.		
54.	1.2.3	Verify that logon capability to accounts bin, lib, uucp, news, sys, guest, daemon, and any default account not normally logged onto is disabled by making the default shell /bin/false, /usr/bin/false, /sbin/false, or /dev/null,	Logon capability to accounts bin, lib, uucp, news, sys, guest, daemon, and any default account not normally logged onto is disabled by making the default shell /bin/false, /usr/bin/false, /sbin/false, or /dev/null, or by		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
		or by disabling the password.	disabling the password.		
55.	17.1.3	Verify that the audit files have permissions of 640, or more restrictive.	Audit files have permissions of 640, or more restrictive.		
56.	17.1.3	Verify that all audit files and directories are readable only by authorized personnel.	All audit files and directories are readable only by authorized personnel.		
57.	17.1.1	Verify that the AUDIT_CONTROL file, at a minimum, audits the following events: logins and logouts, failed file creations, failed file deletions, all administrative actions, failed file writes, failed file modifications (such as chowns and chmods), and system startup and shutdown.	The AUDIT_CONTROL file, at a minimum, audits the following events: logins and logouts, failed file creations, failed file deletions, all administrative actions, failed file writes, failed file modifications (such as chowns and chmods), and system startup and shutdown.		
58.	17.1	Verify that for each audited event the following information is recorded: date and time of the event, userid that initiated the event, type of event, and success or failure of the event.	For each audited event, the correct information is recorded.		
59.	17.1	Verify that the Basic Security Module (BSM) is implemented for auditing on all Sun Solaris systems.	The Basic Security Module (BSM) is implemented for auditing on all Sun Solaris systems.		
60.	1.2.3	Verify that all switch user (su -) attempts are logged to a system log file.	All switch user (su -) attempts are logged to a system log file.		
61.	17.1.3	Verify that the audit_user file has assigned permissions of 640, or more restrictive.	The audit_user file has assigned permissions of 640, or more restrictive.		
62.	1.2.3	Verify that access to cron utilities is controlled using either a cron.allow file or a cron.deny file and that	Access to cron utilities is controlled using either a cron.allow file or a cron.deny file and the contents of the files are		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
		the contents of the files is recorded in system documentation.	recorded in system documentation.		
63.	1.2.3	Verify that either *root* or *bin* own the cron and crontab directories.	Either *root* or *bin* owns the cron and crontab directories.		
64.	1.2.3	Verify that cron logging has been implemented and that the cronlog access permissions are 600, or more restrictive. Verify that cronlogs are included on the same review schedule as other system logs.	Cron logging has been implemented and the cronlog access permissions are 600, or more restrictive. The cronlogs are included on the same review schedule as other system logs.		
65.	1.2.3	Verify that access to *at* is controlled using the at.allow or at.deny file and that contents of the files are recorded in system documentation.	Access to *at* is controlled using the at.allow or at.deny file and contents of the files are recorded in system documentation.		
66.	1.2.3	Verify that the access permissions of the at.allow and at.deny files are 700, or more restrictive.	Access permissions of the at.allow and at.deny files are 700, or more restrictive.		
67.	1.2.3	Verify that access permissions for the *at* (or equivalent) directory are 755, or more restrictive.	Access permissions for the *at* (or equivalent) directory are 755, or more restrictive.		
68.	1.2.3	Verify that the owner and group owner of the *at* (or equivalent) directory is *root*, *bin*, or *sys*.	The owner and group owner of the *at* (or equivalent) directory is *root*, *bin*, or *sys*.		
69.	1.2.3	Verify that default accounts do not appear in the at.allow file and access permissions are 700, or more restrictive.	Default accounts do not appear in the at.allow file and access permissions are 700, or more restrictive.		
70.	16.2.2	Verify that network services that are not necessary for operations are disabled in the inetd.conf file unless justified and documented.	Network services that are not necessary for operations are disabled in the inetd.conf file unless justified and documented.		
71.	16.2.2	Verify that the inetd.conf file is owned	The inetd.conf file is owned by *root* or *bin* and		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
		by *root* or *bin* and has permissions of 440, or more restrictive.	has permissions of 440, or more restrictive		
72.	16.2.2	Verify that anonymous ftp is not configured on systems that are inside the protected perimeter (not in the DMZ), and is only on dedicated machines. The Anonymous ftp server contains no critical information.	Anonymous ftp is not configured on systems that are inside the protected perimeter, is only on dedicated machines, and these machines contain no critical information.		
73.	16.2.2	Verify that unless it is required for business purposes File Transfer Protocol (FTP) is disabled.	File Transfer Protocol (FTP) is disabled unless required for business purposes.		
74.	16.2.2	Verify that File Service Protocol (FSP) is not allowed.	File Service Protocol (FSP) is not allowed.		
75.	16.2.2	Verify that unless it is required for business purposes Trivial File Transfer Protocol (tftp) is disabled.	Trivial File Transfer Protocol (tftp) is disabled unless it is required for business purposes.		
76.	16.2.2	Verify that services to the System Logging Daemon (syslogd) port are restricted to local hosts at the firewall or premise router.	Services to the System Logging Daemon (syslogd) port are restricted to local hosts at the firewall or premise router.		
77.	1.2.3	Verify that the /etc/syslog.conf file is owned by root with access permissions of 640, or more restrictive, and that the group owner is a privileged uid.	The /etc/syslog.conf file is owned by root with access permissions of 640, or more restrictive, and the group owner is a privileged uid.		
78.	16.2.2	Verify that if the machine is not used for routing, the default gateway is defined.	The default gateway is defined if the machine is not used for routing.		
79.	1.2.3	Verify that the TCP_WRAPPERS program, or an equivalent, is implemented on all sensitive or mission	The TCP_WRAPPERS program, or an equivalent, is implemented on all sensitive or mission critical hosts connected		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
		critical hosts connected to a network and that a hosts.deny and hosts.allow file are used.	to a network and a hosts.deny and hosts.allow file are used.		
80.	1.2.3	Ensure that if *sadmind* is not used to remotely manage the Solaris system, it is disabled by deleting or commenting out the requisite line from the inetd.conf file.	If *sadmind* is not used to remotely manage the Solaris system, it is disabled by deleting or commenting out the requisite line from the inetd.conf file.		
81.	10.3.2	Verify that statd and automountd are disabled unless the correct system patch has been applied.	Statd and automountd are disabled unless the correct system patch has been applied.		

Test Number:	SITE:	DATE:
Test Name: Oracle Database Servers		
Resources Required:	All Oracle database servers.	
Personnel Required:	System and Database Administrators with Oracle/System Administrator privileges to the network to be tested, and a System Security Administrator.	
Objectives:	To determine if the Oracle database servers are configured correctly and securely.	
Procedure Description:(Summary)	Review system settings on the Oracle database servers. Interview System and Database Administrators and System Security Administrators.	

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
1.	1.2.3	Check to ensure that the *seuid* bit is disabled on appropriate directories.	All sensitive system directories have the *seuid* bit set to disabled.		
2.	1.2.3	Verify that if the Oracle Security Server is used for authentication, the appropriate directories are secured.	All sensitive system directories have appropriate permissions assigned.		
3.	1.2.3	Verify that the Oracle *OS_AUTHENT_PREFIX* setting is set to something other than *OPS$*.	The setting has been changed from the default system setting.		
4.	1.2.3	Verify that Oracle database *link password encryption* is enabled.	*Link password encryption* is used.		
5.	1.2.3	Verify that Oracle databases running on Windows NT/2000 servers have registry permissions set correctly.	Operating system registry entries have appropriate registry permissions assigned.		
6.	11.2.3	Verify the default *Listener* password is changed (not default or blank).	The default *Listener* password has been changed.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
7.	1.2.3	Verify that Oracle databases are configured to encrypt all data transmitted between a client computer and an Oracle instance using the secure socket layer (SSL) or Transport Layer Security (TLS) protocol.	All data transmitted between client computers and Oracle instances is encrypted via SSL or TLS.		
8.	10.3.2	Verify that the Oracle Intelligent Agent patch is installed.	The Intelligent Agent patch is installed.		
9.	1.2.3	Verify that Oracle files do not have the *setgid* bit enabled.	Sensitive Oracle system files do not have the *setgid* bit enabled.		
10.	11.2.3	Verify that installations using Oracle 8.0 and later employ the use of the Oracle password verification script in order to enforce password complexity.	Installations using version 8.0 and later employ the use of the Oracle password verification script and enforce password complexity.		
11.	11.2.3	Verify that Oracle 7 servers are manually checked at scheduled intervals for expired passwords.	All Oracle 7 servers are manually checked for expired passwords at scheduled intervals.		
12.	1.2.3	Verify that all sensitive Oracle system files are owned by the Oracle software owner account.	All sensitive Oracle system files are owned by the Oracle software owner account.		
13.	15.1.6	Verify that Oracle 8 and later installations have passwords set to expire after 90 days.	Oracle passwords expire after 90 days.		
14.	15.2.2	Ensure that privileged OS users are restricted.	Use of privileged accounts is restricted.		
15.	1.2.3	Verify that Oracle 8.0 and earlier versions on Windows NT/2000 have placed appropriate restrictions on the Oracle startup file.	Proper permissions are assigned to the startup file.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
16.	16.2.3	Verify that the Oracle *Internal Password* has been changed from the default installation password.	The default *Internal Password* has been changed.		
17.	16.2.4	Verify that the Oracle remote login password file complies with the current Oracle system policy.	The remote login password file complies with the existing Oracle system policy.		
18.	16.1.1	Ensure that auditing of failed connections to Oracle databases is enabled and that the auditing data is written to the *SYS.AUD$* table or to the OS logs and that manual checks of password attacks occur.	Failed connections are logged and manual checks of password attacks are performed.		
19.	15.1.7	Verify that Oracle is not using weak SNMP passwords.	Oracle SNMP passwords comply with written password complexity policies.		
20.	11.2.3	Ensure that the default Oracle SNMP and Account passwords have been changed.	All default SNMP and account passwords have been changed.		
21.	11.2.3	Verify that the *Administrative Restrictions Listener* is set to ON and a strong *listener* password has been established.	The *Administrative Restrictions Listener* is enabled and a strong password has been established.		
22.	17.1.3	Ensure that permissions to the Oracle *Audit Table* are restricted to only those requiring access.	Only those accounts tasked with auditing duties have access to the *Audit Table*.		
23.	11.2.3	Verify that the Oracle SNMP files have appropriate permissions.	SNMP files have appropriate permissions set.		
24.	17.1.3	Ensure that access to the Oracle UTL_FILE package is restricted.	Access to the file is restricted to Database Administrators.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
25.		Verify that Oracle licensing is compliant with the maximum amount of expected concurrent users.	An approximate estimate of the maximum amount of concurrent connections exists and the estimate complies with the number of licenses purchased.		
26.	1.2.3	Ensure that installations of Oracle 8.0 have restricted *Dictionary Accessibility*.	*Dictionary Accessibility* is restricted.		
27.	11.2.3	Verify that all Oracle roles with access to sensitive data have passwords assigned to them.	All Oracle roles with access to sensitive data have passwords assigned to them.		
28.	11.2.3	Ensure that password reuse restrictions in Oracle 8 are enabled.	Password reuse restrictions are enabled.		
29.	11.2.3	Verify that the Oracle *Internal Password* that is logged during install has been deleted.	The *Internal Password* entry has been removed.		
30.	11.2.1	Ensure that file checksums for files located in sensitive directories have been created and are monitored for changes.	File checksums have been created and files are monitored for changes.		
31.	1.2.3	Verify that the Oracle *Listener* is filtered at all border gateways.	All border gateways filter the Oracle *Listener*.		
32.	1.2.3	Verify that *Valid Node Checking* is enabled.	*Valid Node Checking* has been enabled.		

Test Number:	SITE:	DATE:
Test Name: Data Integrity and Confidentiality		
Resources Required:	Documentation and procedures for malicious code control as they relate to the operation of [SYSTEM NAME].	
Personnel Required:	[SYSTEM NAME] systems personnel tasked with malicious code control.	
Objectives:	The objectives of this test are to determine the degree of compliance with applicable Federal and HUD requirements for malicious code control on [SYSTEM NAME].	
Procedure Description: (Summary)	Interview personnel and review documentation and procedures related to malicious code control for [SYSTEM NAME] and testing of malicious code programs on selected computers.	

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
1.	11.1	Is anti-virus/malicious code software installed?	Anti-virus software is installed (applies primarily to Windows-based systems).		
2.	11.1.1	Is date of virus signatures on anti-virus configuration window less than four weeks old?	Date indicates signatures are no more than four weeks old.		
3.	11.1.1	Is software set for "Auto-Protect" or scheduled to run full scans at specific intervals, no longer than once a week?	Settings are configured according to IBPs.		
4.	11.1.1	Are virus scans of all drives being performed on a regular basis?	Drives are scanned regularly.		
5.	9.1.1	Are data and system backups accomplished on a regular basis?	The agency has established a schedule of routine data and system backups.		
6.	9.1.1	If a Redundant Array of Inexpensive Disks (RAID) is used on sensitive or mission critical systems, is it RAID-5 level or better?	RAID 5 is used.		
7.	11.2.4	Do sensitive or mission critical systems employ a file integrity system?	A file integrity system is provided by the operating system or from an authorized tested add-on product (i.e. tripwire).		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
8.	16.1.7	Is encryption used on non-Departmental networks, public switched networks, and the Internet?	Encryption is used on external communication paths.		
9.	16.1.8	Are passwords encrypted during transmission?	The operating system provides for hashing or encryption of passwords when transmitted.		
10.	16.1.7	Are PKI private keys (if used) stored in an encrypted form?	Private keys are stored on an encrypted database or hard drive.		
11.	16.1.7	Are laptops provided with encryption methods to protect data stored on the laptop's hard drive?	Laptops employ native operating system or third party add-on file encryption software.		
12.	15.1.2	Are all encryption techniques used FIPS compliant?	All encryption software and hardware on the network or for individual user use is FIPS compliant.		

Test Number:	SITE:	DATE:
Test Name: IIS & ASP Servers		
Resources Required:	All Internet and Intranet web servers running IIS or active server pages.	
Personnel Required:	Web Administrators with Web Administrator privileges for the network to be tested, and a Network Security Administrator.	
Objectives:	To determine if the web servers are configured correctly and securely.	
Procedure Description:(Summary)	Review system settings on the Web Servers. Interview Web Administrators and Network Security Administrators.	

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
1.	3.1.6	Are the appropriate virtual directory permissions and Web application spaces set?	Virtual directories and Web application spaces have correct permissions assigned.		
2.	16.2.2	Are non-trusted Root Certificates removed and Secure Sockets Layer (SSL) or Transport Layer Security (TLS) used, if applicable?	Non-trusted Root Certificates have been removed and SSL or TLS is used to protect sensitive information in transit.		
3.	1.2.3	Are Access Control Lists (ACLs) set appropriately on IIS log files?	IIS log files have appropriate permissions set in the ACLs.		
4.	1.2.3	Is W3C Extended Logging Format being used to audit for in-depth information?	W3C Extending Logging format is employed.		
5.	1.2.3	Are Certificate Server ASP Enrollment pages (if not used) removed, or are ACLs set?	Either the Certificate Server ASP enrollment pages are removed or the ACLs are configured correctly.		
6.	1.2.3	Is the IISADMPWD virtual directory removed, if not needed?	The IISADMPWD directory has been removed or restricted via ACLs.		
7.	1.2.3	Are parent paths disabled?	Parent paths are disabled.		
8.	1.2.3	Is IP Address disabled in Content-Location?	The IP address is not listed in Content-Location.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
9.	1.2.3	Does IIS Global.asp contain no identification information, and is it protected?	The Global.asp file contains no information and is appropriately restricted.		
10.	1.2.3	Is IIS Showcode.asp removed?	Showcode.asp has been removed.		
11.	1.2.3	Does the IIS ASP implementation employ methods for proper bounds checking?	Proper bounds checking is employed in ASP server pages.		
12.	1.2.3	Is the IIS Metabase backed up regularly, stored in a protected area, and tested for restoration ability?	The IIS Metabase is backed-up regularly, stored in a protected area, and tested for restoration ability.		
13.	1.2.3	Has the IIS Lockdown tool been used to secure IIS servers?	The IIS Lockdown tool has been used to secure the IIS server.		
14.	16.2.2	Is the Internet Printing Protocol disabled on IIS servers?	The Internet Printing Protocol has been disabled.		
15.	16.2.2	Is IIS Remote Data Services (RDS) disabled?	IIS RDS is disabled.		
16.	1.2.3	Are the unused IIS script mappings removed?	All unused script mappings are removed.		
17.	1.2.3	Are IIS permissions synchronized with NTFS file permissions?	IIS permissions (ACLs) are synchronized with NTFS file permissions.		
18.	1.2.3	Does the IIS installation use security templates, such as hisecWeb.inf, modified for organizational needs?	Modified high-security templates have been employed on production IIS web servers.		
19.	1.2.3	Have utilities restricting the type of http requests that web servers may process been implemented? (E.g., URLscan)	Utilities restricting the types of URLs that web servers may process have been employed.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
20.	8.2.1	Do Internet web sites that process sensitive client/customer data offer some measure of compliance with industry best practices for safeguarding a customer's personal data and information?	Data and information concerning customers is secured and protected according to industry best practices.		
21.	1.2.3	Does the Web site have a valid Digital Certificate to prove the information presented in the web page originated from the organization's servers?	A digital certificate containing accurate information is used for communications (SSL or TLS).		
22.	1.2.3	Is the SSL encryption at least 128-bit with 1024 bit keys?	SSL/TLS sessions are 128-bit with 1024-bit keys.		
23.	16.1.7	Is there support for browsers not supporting 128-bit SSL encryption?	Server Gated Cryptography is supported by the digital certificate.		
24.	1.2.3	Do Microsoft® ASP applications protect against cross-site scripting attacks via input filtering?	Inputs to web pages are checked for proper formatting.		
25.	1.2.3	Are there cookies stored in the IIS log if they are persistently used?	The IIS log does not store persistent cookies.		
26.	1.2.3	Are users required to login each time they use an online application?	Users are required to log into the application for each new session.		
27.	1.2.3	Is the Microsoft® Internet Explorer Auto-complete feature disabled via server-side attributes?	Auto complete is disabled.		
28.	16.2.6	Are users logged out as soon as they leave a web site and/or online application?	Users are logged out as soon as they leave the web site.		
29.	15.1.8	Are online sessions disconnected if they are inactive for 30 minutes?	Inactive sessions are disconnected after 30 minutes.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
30.	1.2.3	Does the application code prevent simultaneous logins?	Applications prevent simultaneous logins.		
31.	1.2.3	Does the application code used on production servers contain developer comments?	All developer comments are removed from production code contained on production servers.		

Test Number:	SITE:	DATE:
Test Name: SQL Servers		
Resources Required:	All SQL Servers.	
Personnel Required:	Database Administrators with Database Administrator privileges for the network to be tested, and a Network Security Administrator.	
Objectives:	To determine if the database servers are configured correctly and securely.	
Procedure Description:(Summary)	Review system settings on the SQL Servers. Interview Database Administrators and Network Security Administrators.	

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
1.	3.1.6	Verify all SQL Patches, Service Packs and hotfixes have been identified, installed and tracked for each server.	All patches and service packs are up to date.		
2.	16.2.2	Is Secure Sockets Layer (SSL) or Transport Layer Security (TLS) used for sensitive communications between servers and clients?	SSL and or TLS is used for secure communication between the server and client.		
3.	1.2.3	Ensure the “sa” and “probe” (SQL 6.5) accounts are secured with strong passwords, and that the passwords are stored in a secure location. Note: The probe account is used for performance analysis and distributed transactions. Assigning a password to this account can break functionality when used in standard security mode.	The “sa” and “probe” accounts are secured with strong passwords and the passwords are stored in a secure location.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
4.	1.2.3	Verify a low-privilege user account is used for SQL Server service rather than LocalSystem or Administrator.	A low-privilege user account is used for SQL Server services.		
5.	1.2.3	If not needed, the extended process command shell (master.xp_cmdshell) and all the OLE automation stored procedures have been denied EXECUTE permission except for specific users and/or roles.	The extended process command shell and all the OLE automation stored procedures have been denied EXECUTE permissions except those required for specific users and/or roles.		
6.	1.2.3	Verify all unneeded OLE automation stored procedures been removed.	All unneeded OLE automation stored procedures have been removed.		
7.	1.2.3	Verify all unneeded registry access procedures have been removed.	All unneeded registry access procedures have been removed.		
8.	1.2.3	Verify all other unneeded system stored procedures have been removed.	All unneeded system stored procedures have been removed.		
9.	1.2.3	Verify the Guest user has been removed.	The Guest user account has been removed.		
10	1.2.3	Unless needed, ensure the SQL Mail service been disabled.	The SQL mail service has been disabled.		
11	1.2.3	Verify logging for all user access to sensitive systems has been enabled. Ensure that all Administrator or privileged user access is audited.	Logging and auditing is enabled for users and administrators.		
12	1.2.3	Verify that database applications been written to use user-defined stored procedures and views whenever possible, and that general access to tables has been limited.	Database applications have been written to user-defined stored procedures and views and general access to tables has been limited.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
13	1.2.3	Verify the SELECT, INSERT, UPDATE and DELETE commands contained within stored procedures allow only applications to call the stored procedures instead of directly accessing the commands.	The commands contained within the stored procedures allow only applications to call the stored procedures.		
14	16.2.2	Ensure that failed access to objects, files, and tables is monitored.	Failed access to objects, files, and tables is monitored.		
15	16.2.2	Verify that thresholds have been set and that administrators are notified of events automatically	Thresholds have been set and administrators are notified of events automatically.		
16	1.2.3	Verify that change control/ configuration management procedures is followed for database software and hardware modifications.	Change control/ configuration management procedures are used for database software and hardware modifications.		
17	1.2.3	Verify that database groups and roles are routinely audited to ensure the level of access is only what is needed for job-related functions and tasks.	Database groups and roles are routinely audited to verify the level of access.		
18	1.2.3	Verify that the appropriate ACLs are set for database system files, database administrative tools, database system registry entries, and database files that control security services.	The appropriate ACLs are set for all files.		
19	1.2.3	Verify that the PUBLIC group is restricted from issuing SELECT statements.	The PUBLIC group is restricted from issuing SELECT statements.		
20	8.2.1	Verify that database accounts are (logins) routinely checked for null passwords.	Database login accounts are checked for the use of null passwords.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
21	1.2.3	Verify that integrated security (operating system or Windows Authentication Mode) is used.	The integrated security operating system or Windows Authentication Mode is used.		
22	1.2.3	If integrated security is used, verify that the sa password has been removed from the registry.	The sa password has been removed from the registry.		
23	16.1.7	Verify that database procedures are routinely queried to limit the number of procedures with PUBLIC access.	Database procedures are routinely queried.		
24	1.2.3	Verify that interactive logins to the database server are restricted.	Interactive logins to the database server are restricted.		
25	1.2.3	Verify that unused ODBC/OLE-DB database drivers and unnecessary Component Object Module (COM) components have been removed.	All unnecessary ODBC/ODE-DB database drivers and unnecessary COM components have been removed.		
26	1.2.3	Ensure file and disk shares are read-only (RO) by default and are only changed on an as-needed basis.	File and disk shares are read-only.		
27	1.2.3	Verify that the database server is isolated from the Internet.	A firewall is installed that isolates the database server from the Internet.		
28	16.2.6	If operationally possible, ensure the SQL Server service is hidden from being enumerated by the Query Analyzer.	The SQL Server service is hidden from being enumerated by the Query Analyzer.		
29	15.1.8	Verify that secure links are used for database replication (VPNs) when replication occurs over public or mistrusted networks.	VPNs are used for replication.		

Step #	NIST 800-26 Element ID	Procedure Description	Expected Results	Actual Results	P, F, N/A
30	1.2.3	Verify that access to the snapshot folder is restricted to only the replication agents.	Access to the snapshot folder is restricted to only the replication agents.		
31	1.2.3	Verify that the Microsoft SQL Server 2000 backup service requires a password for access.	The MS SQL Server 2000 backup service requires a password.		
32	1.2.3	Verify that Valid Node Checking is enabled.	Valid Node Checking is enabled.		

Appendix B – Document Evidence

This section is for screen shots and other documentation. If you have more than one, entitle each "Attachment 1 (kind of evidence)" etc.

Appendix C – Vulnerability Assessment Report

Cut and paste automated vulnerability scan results here.

INDEX