DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

Information Security Program

Information Technology Security Test and Evaluation Guide

August 24, 2005

SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Table of Contents

Preface

As the Department of Health and Human Services (HHS) Information Technology Security Program evolves, this document will be subject to review and update, which will occur annually or when changes occur that signal the need to revise the *HHS Information Technology (IT) Security Test and Evaluation (ST&E) Guide*. These changes may include the following:

- Changes in roles and responsibilities;
- Release of new executive, legislative, technical, or Departmental guidance;
- Identification of changes in governing policies;
- Changes in vulnerabilities, risks or threats; and/or
- HHS Inspector General findings that stem from a security audit.

The HHS Chief Security Officer (CSO) must approve all revisions to the *HHS IT ST&E Guide*. Revisions are to be highlighted in the Document Change History table. Each revised guidance document is subject to HHS' document review and approval process before becoming final. When it is approved, a new version of the *HHS IT ST&E Guide* will be issued, and all affected parties will be informed of the changes made.

The procedures outlined in the *HHS Security Test and Evaluation Guide* are proven practices that will provide guidance to the Department in meeting or exceeding the mandatory policies identified in the *HHS Information Security Program Policy* document. The *HHS Security Test and Evaluation Guide* provides specific information for the recommended implementation of testing and evaluation procedures. While the specifics of how to undertake the implementation are not mandatory, any security implementation undertaken by an OPDIV must result in security controls and processes that are equal to or stronger than those articulated in the Policies, Handbooks, and related Guides. If an OPDIV or STAFFDIV chooses not to adopt the baseline guidance set forth in this *HHS Security Test and Evaluation Guide*, it must document this decision and assume responsibility for the creation of procedures of equal or greater stringency.

Document Change History

Version Number	Release Date	Summary of Changes	Section Number / Paragraph Number	Changes Made By
1.0	01/12/2005	Final Release	NA	NA
1.1	06/22/2005	Incorporated OPDIV feedback	Throughout	HHS CSO
2.0	08/24/2005	Updated to reflect new HHS guidance and regulatory requirements	Throughout	NA

1. Introduction

The Department of Health and Human Services (HHS) is responsible for implementing and administering an information security program to protect its information resources, in compliance with applicable public laws, federal regulations, and executive orders, including the *Federal Information Security Management Act of 2002* (FISMA); the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, dated November 28, 2000; and the *Health Insurance Portability and Accountability Act of 1996* (HIPAA). To meet these requirements, the Department has instituted the *HHS Information Security Program Policy* document and accompanying *HHS Information Security Program Handbook* document.

The *HHS Information Technology (IT) Security Test and Evaluation (ST&E) Guide* was created as part of the HHS Information Security Program to act as a guide for developing and executing an ST&E process that can be implemented consistently across the Department. This guide is in accordance with the guidelines set forth in the *HHS Information Security Program Policy*, OMB Circular A-130, and other applicable federal IT security laws and regulations.

1.1 Purpose

This ST&E guide provides an overview of the role of ST&E as it relates to the certification and accreditation (C&A) of all Departmental general support systems (GSS) and major applications (MA) whose certification impact falls in the moderate- or high-impact areas of the certification level of effort. This guide establishes Departmental parameters and minimum standards for an ST&E, which meet the requirements of the *HHS Information Security Program Certification and Accreditation Guide*.

1.2 Background

ST&E is an examination and analysis of both technical and nontechnical security safeguards of IT resources as they have been applied in an operational environment. The ST&E process includes developing an ST&E Plan, executing the ST&E Plan, and developing the ST&E Report. The ST&E Report will serve as input to the Certification Authority (CA) and Designated Approving Authority (DAA) to help them make the accreditation decision for Departmental GSSs and MAs.

This guide explains why security testing is important, how an ST&E feeds into the C&A process, and the methodology for conducting an ST&E. An ST&E, as described in this guide, is required for all information systems that fall into the moderate- or high-impact areas of the certification level of effort[1].

The Department developed this guide to meet the security requirements set forth in the following documents/standards:

- *HHS Certification and Accreditation Guide*. An ST&E is a required activity for all moderate or high certification level of effort systems undergoing C&A. The ST&E will assess the technical implementation of the security design, ensure that the security controls have been implemented as necessary, and ensure that the features perform as planned. The result is the ST&E Report, which is part of the required C&A security documentation.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*. System security testing assesses the effectiveness of the security controls of an IT system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.
- NIST SP 800-36, *Guide to Selecting Information Security Products.* Independent, third-party testing and evaluation of IT products gives consumers greater confidence that the security features in those products work as advertised by the vendor. The evidence produced during the product testing and evaluation process (available in different forms depending on the program) can be used by system integrators to build more secure systems and networks. System certifiers can also use this evidence to more effectively assess the security of an IT system in its operational environment in support of system accreditation.
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems.* The information security program must include periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls. This testing should be performed with a frequency depending on risk, but no less than annually.
- NIST SP 800-42, *Guide on Network Security Testing.* Security testing is perhaps the most conclusive determinant of whether a system is configured to the correct security controls and policies.
- OMB Circular A-130, *Management of Federal Information Resources.* The protection of government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information is required of all federal agencies.

[1] See the *HHS Information Security Program Certification and Accreditation Guide* for information regarding the certification impact and level of effort categorization.

1.3 Scope

This guide is written with the assumption that the reader possesses basic IT security knowledge and associated disciplines in security testing. The personnel responsible for the security of Departmental GSSs and MAs (e.g., Chief Information Security Officer (CISO), Information Systems Security Officer (ISSO), system owners, and system/network administrators) should use this guide to obtain an understanding of the objectives and importance of conducting an ST&E and the methodology for conducting that ST&E. This guide is intended to explain the ST&E process. It does not address or describe vulnerability scanning or penetration testing.

1.4 Document Organization

The remainder of this guide is structured as follows:

- Section 2 introduces the ST&E process.
- Section 3 describes how an ST&E is conducted.
- Section 4 summarizes the points of this guide.

This guide also contains the following appendices:

- Appendix A provides a feedback form for use in submitting comments on this document to HHS.
- Appendix B lists the references used in this document.
- Appendix C lists the acronyms used in this document.
- Appendix D defines terms most frequently used in this document.
- Appendix E provides an ST&E Plan template.
- Appendix F provides an ST&E Report template.
- Appendix G provides a list of the documents associated with the HHS Information Security Program.

2. Security Test and Evaluation Overview

An ST&E is performed to satisfy OMB A-130, Appendix III requirements that executive agencies periodically review the security controls in their information systems. Testing is a fundamental security activity that can be conducted to achieve a secure operating environment while fulfilling the Department's security requirements. ST&E allows HHS and Operating Divisions (OPDIV) to accurately assess their system's security posture. This section provides a description and addresses the objectives of ST&E, discusses the frequency for performing ST&E, provides a description of the types of security controls to be tested, defines participating individuals and their associated responsibilities, describes ST&E as related to C&A, and provides the various levels of effort for testing.

2.1 Objectives

The objectives of the ST&E are to:

- Uncover design, implementation, and operational flaws that could allow the violation of security policies that may affect the confidentiality, integrity, and availability of the information and information systems;
- Determine the adequacy of security mechanisms, assurances, and other properties to enforce the Department's security policy; and
- Assess the degree of consistency between the system documentation and its implementation.

2.2 Frequency

The ST&E is conducted as part of the C&A process for a new system, before it goes into operations, or as part of an existing system, at least every three years or when a significant change has been made to the system. As outlined in the *HHS Certification and Accreditation Guide,* an ST&E should be conducted as part of Phase 2: Security Certification of the Departmental C&A process. This will assist in validating that appropriate management, operational, and technical security controls have been implemented for the information system. The ST&E is generally conducted after the risk assessment to ensure that the security weaknesses identified as part of the risk assessment have been resolved and/or mitigated.

2.3 What Should Be Tested?

Testing should be performed on all hardware and software components to ensure that all Departmental baseline security controls are adequately addressed. Security controls are divided into three classes, as defined in Table 1.

Table 1. Definition of Security Domains

Class	Definition
Management Controls	The security controls (i.e., safeguards or countermeasures) for an information system that focus on risk management and managing information system security.
Operational Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
Technical Controls	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Three sets of minimum (baseline) controls are identified in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. Each set of controls corresponds to the low-, moderate-, and high-impact levels defined in the security categorization process in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*.

2.4 Roles & Responsibilities

A number of individuals play integral roles in the ST&E process. The primary individuals associated with the ST&E process are individuals on the ST&E team and the system owner.

2.4.1 HHS Chief Security Officer and OPDIV Chief Information Security Officers

The HHS Chief Security Officer (CSO) and OPDIV CISOs are responsible for the following activities associated with security testing:

- Ensuring the development and implementation of security policies, standards, and procedures for their area of responsibility;
- Ensuring compliance with security policies, standards, procedures, and requirements; and
- Ensuring that critical systems are identified and scheduled for periodic testing according to the security policy requirements of each respective system.

2.4.2 Information System Security Officer

The HHS and OPDIVs ISSOs are responsible for the following activities associated with security testing:

- Developing security standards and procedures for their area of responsibility;

- Assisting in developing and implementing security tools and mechanisms;
- Maintaining configuration profiles of all systems controlled by the organization, including but not limited to, mainframes, distributed systems, microcomputers, and dial access ports; and
- Maintaining operational integrity of systems by conducting tests and ensuring that designated IT professionals are conducting scheduled testing on critical systems.

2.4.3 System and Network Administrators

The HHS and OPDIV IT administrators are responsible for the following activities associated with security testing:

- Monitoring system integrity, protection levels, and security-related events;
- Following up on detected security anomalies associated with their information system resources; and
- Executing security tests as required.

2.4.4 ST&E Team

The ST&E team should consist of independent third-party individual(s) to develop and execute test procedures. To be considered independent, members of the ST&E team should not have a vested interest in the development or documentation of the system. ST&E team members should have significant system testing experience and should be selected based on their understanding of the system that is undergoing security testing and the depth of testing required. Utilizing individuals with specific system knowledge ensures that security vulnerabilities are appropriately addressed and adequately tested. The ST&E team is responsible for the following activities associated with security testing:

- Developing the ST&E Plan;
- Executing the ST&E; and
- Documenting test results after each procedure in an ST&E Report.

For low-impact systems, the information system owner may employ the services of the information system security officer or other designated individuals (including contractors) to conduct a self-assessment of the information system security controls. An independent certification agent is not required to participate in the process (see NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* section 3.2, for further details).

2.4.5 System Owner

The HHS and OPDIVs system owners are responsible for the following activities associated with security testing:

- Working closely with the ST&E team to determine the components to be tested and to ensure that the components are operational at the time of testing;
- Providing the ST&E team with the necessary system documentation (e.g., system diagram, system security plan, configuration management plan (CMP), contingency plan, requirements documentation, risk assessment) to ensure that the GSS or MA components are identified and available for testing;
- Ensuring that the required personnel (i.e., network, system, and database administrators) are available to assist with testing. However, to avoid potential conflicts of interest, system developers, software designers, or other parties with a vested interest should not be a part of performing the ST&E;
- Overseeing the overall compliance of their systems with their defined/identified security requirements; and
- Ensuring that test results and recommendations are adopted as appropriate.

2.5 The ST&E and C&A Relationship

The C&A process is comprised of the following four phases: Phase 1: Initiation; Phase 2: Security Certification; Phase 3: Security Accreditation; and Phase 4: Continuous Monitoring. ST&E activities take place during Phase 2: Security Certification. The ST&E team for the system will first develop the ST&E Plan. Then, the system owner will review the ST&E Plan and procedures to ensure that they are executable. Finally, the ST&E team will conduct testing by executing the ST&E Plan. The results of the ST&E will be used in validating that management, operational, and technical security controls have been implemented for the system according to the ST&E Plan. The ST&E will also provide assurance that security weaknesses identified as part of the risk assessment of the system have been resolved and that the risks have been properly mitigated. ST&E testing procedures will be developed for each observation identified as a result of the risk assessment. The ST&E team will document the ST&E results in the ST&E Report, which will serve as supporting documentation to the CA and DAA to determine the certification and accreditation decision.

2.6 Determining the Certification Level of Effort

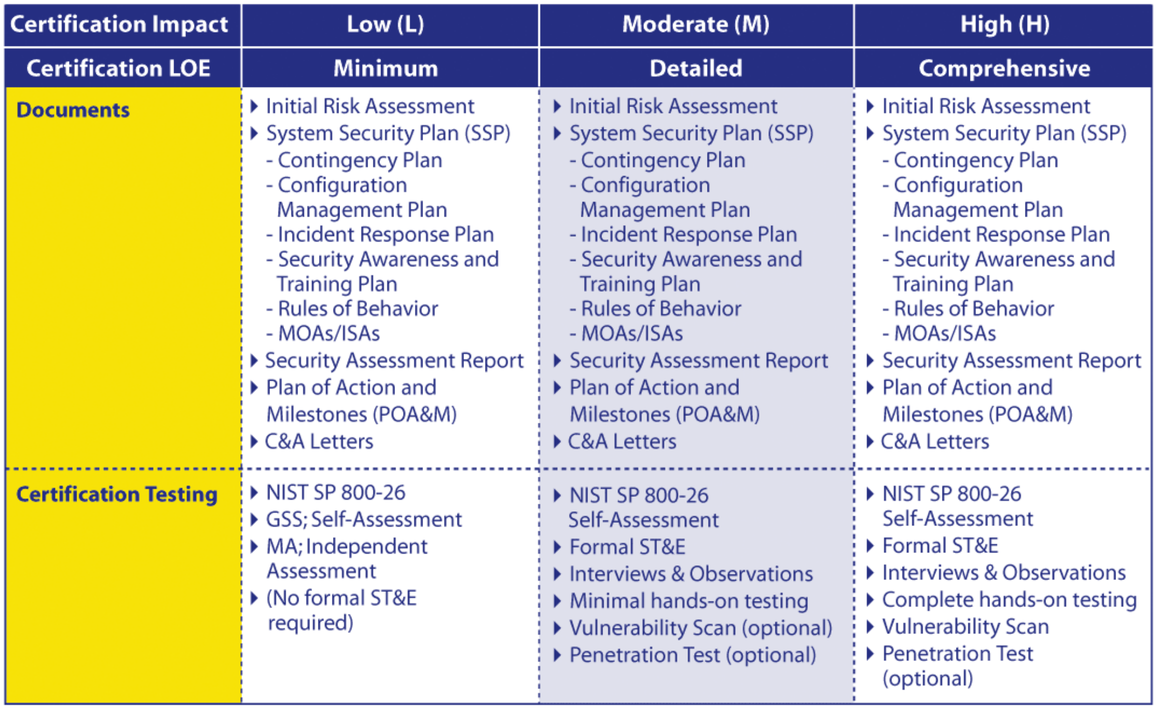
Each information system will be categorized into one of three certification level of effort impact areas (as listed in Table 2). The certification impact area of the information system will determine the certification level of effort[2] required for completing C&A. If an information system falls in the moderate- or high-impact area, the certification level of effort requires that an ST&E be conducted.

The certification impact is determined by analyzing the information system mission and the information stored as it relates to the criticality to HHS and its mission. The certification impact is also influenced by the system's sensitivity, including the confidentiality, integrity,

[2] See the *HHS Information Security Program Risk Assessment Guide* for more information regarding level of effort.

and availability of system data. Systems that fall into the moderate- or high-impact area are considered critical and sensitive systems; therefore, these systems require ST&Es. As shown in the table below, low-impact systems do not require ST&E.

Table 2. ST&E Levels of Effort by Certification Impact

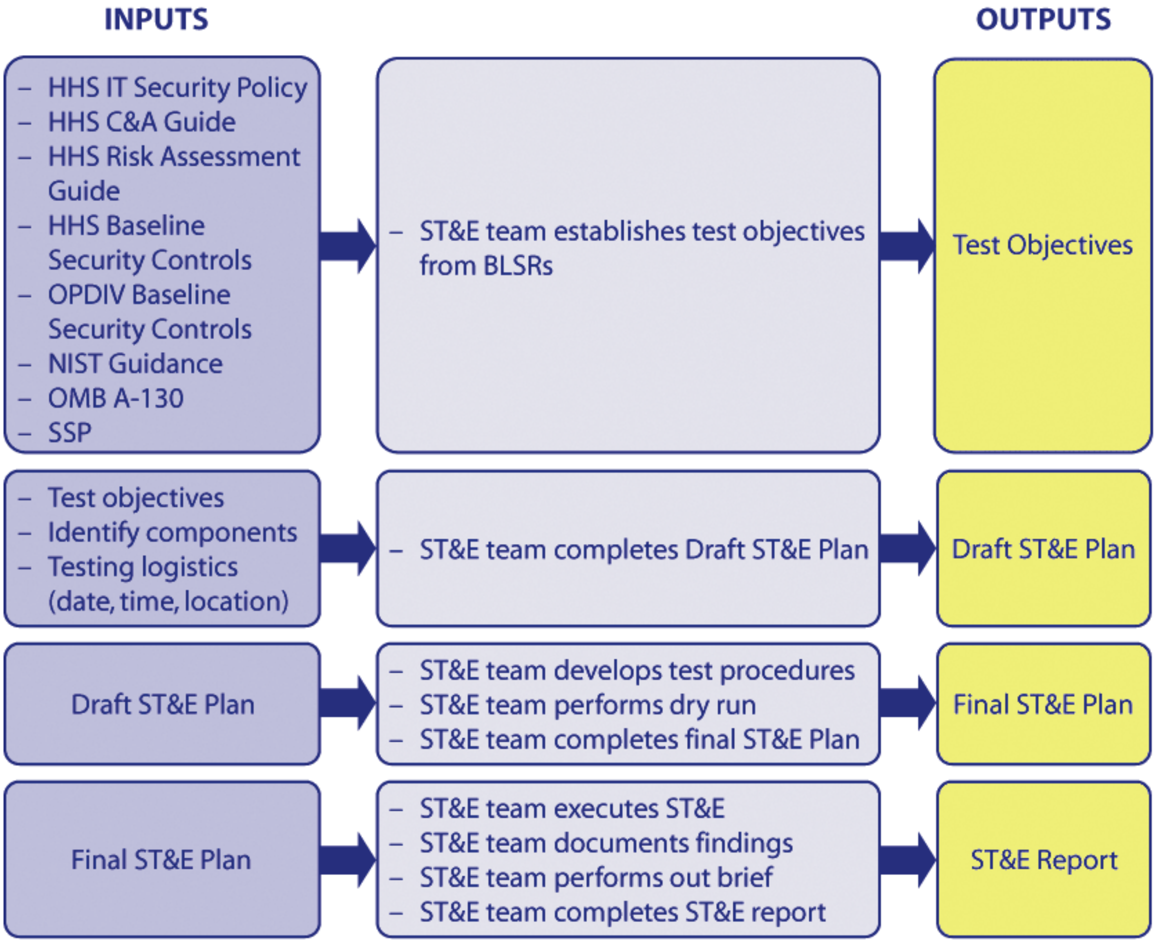


Certification Impact	Low (L)	Moderate (M)	High (H)
Certification LOE	Minimum	Detailed	Comprehensive
Documents	▸ Initial Risk Assessment ▸ System Security Plan (SSP) - Contingency Plan - Configuration Management Plan - Incident Response Plan - Security Awareness and Training Plan - Rules of Behavior - MOAs/ISAs ▸ Security Assessment Report ▸ Plan of Action and Milestones (POA&M) ▸ C&A Letters	▸ Initial Risk Assessment ▸ System Security Plan (SSP) - Contingency Plan - Configuration Management Plan - Incident Response Plan - Security Awareness and Training Plan - Rules of Behavior - MOAs/ISAs ▸ Security Assessment Report ▸ Plan of Action and Milestones (POA&M) ▸ C&A Letters	▸ Initial Risk Assessment ▸ System Security Plan (SSP) - Contingency Plan - Configuration Management Plan - Incident Response Plan - Security Awareness and Training Plan - Rules of Behavior - MOAs/ISAs ▸ Security Assessment Report ▸ Plan of Action and Milestones (POA&M) ▸ C&A Letters
Certification Testing	▸ NIST SP 800-26 ▸ GSS; Self-Assessment ▸ MA; Independent Assessment ▸ (No formal ST&E required)	▸ NIST SP 800-26 Self-Assessment ▸ Formal ST&E ▸ Interviews & Observations ▸ Minimal hands-on testing ▸ Vulnerability Scan (optional) ▸ Penetration Test (optional)	▸ NIST SP 800-26 Self-Assessment ▸ Formal ST&E ▸ Interviews & Observations ▸ Complete hands-on testing ▸ Vulnerability Scan ▸ Penetration Test (optional)

3. Security Test and Evaluation Methodology

Through hands-on testing, interviews, and documentation review, the ST&E activities access security requirements of an information system. A primary goal of ST&E is to verify that the system configuration and operational environment is compliant with the baseline security controls. To realize this goal an ST&E Plan is developed, executed, and completed in a formal ST&E Report using the methodology described in Figure 1. The ST&E methodology presented here should not, however, preclude immediate remediation activities for critical vulnerabilities discovered during the ST&E process.

Figure 1 presents the multi-step ST&E methodology that will be followed to develop and execute the ST&E Plan as well as develop the ST&E Report. Inputs, major activities (including the responsible parties), and outputs for each step are represented in the figure.



INPUTS		OUTPUTS
– HHS IT Security Policy – HHS C&A Guide – HHS Risk Assessment Guide – HHS Baseline Security Controls – OPDIV Baseline Security Controls – NIST Guidance – OMB A-130 – SSP	– ST&E team establishes test objectives from BLSRs	Test Objectives
– Test objectives – Identify components – Testing logistics (date, time, location)	– ST&E team completes Draft ST&E Plan	Draft ST&E Plan
Draft ST&E Plan	– ST&E team develops test procedures – ST&E team performs dry run – ST&E team completes final ST&E Plan	Final ST&E Plan
Final ST&E Plan	– ST&E team executes ST&E – ST&E team documents findings – ST&E team performs out brief – ST&E team completes ST&E report	ST&E Report

Figure 1. ST&E Methodology

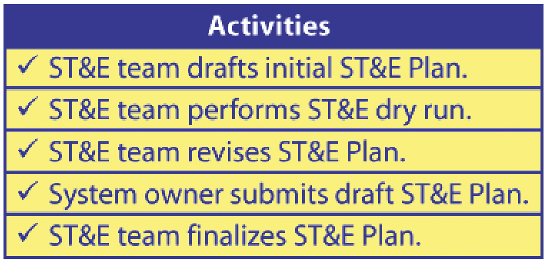
3.1 Step 1: Establish Test Objectives

Test objectives are statements that are derived from HHS Baseline Security Requirements (BLSR) as documented in the *HHS Baseline Security Requirements Guide*. These objectives are created to verify the existence of security controls to ensure that adequate security practices and procedures are in place to protect the information system. The ST&E team will use the test objectives to determine if a system, in it's operational environment, and with the required security controls in place, satisfies a BLSR. This will ensure that the controls used to mitigate system weaknesses are properly implemented.

3.2 Step 2: Develop Initial ST&E Plan

Step 2 establishes the outline and scope of the ST&E Plan. The ST&E Plan will include all test objectives, procedures, and execution processes to be initiated during testing. The ST&E Plan will include a separate set of test procedures for each component identified from the information system documentation. The initial draft ST&E Plan the ST&E team created will include complete test procedures for management, operational, and technical controls[3]. The system owner may work with the ST&E team to identify system components and finalize the plan. Table 3 identifies the ST&E Plan activities.

Table 3. ST&E Plan Activities



Activities
✓ ST&E team drafts initial ST&E Plan.
✓ ST&E team performs ST&E dry run.
✓ ST&E team revises ST&E Plan.
✓ System owner submits draft ST&E Plan.
✓ ST&E team finalizes ST&E Plan.

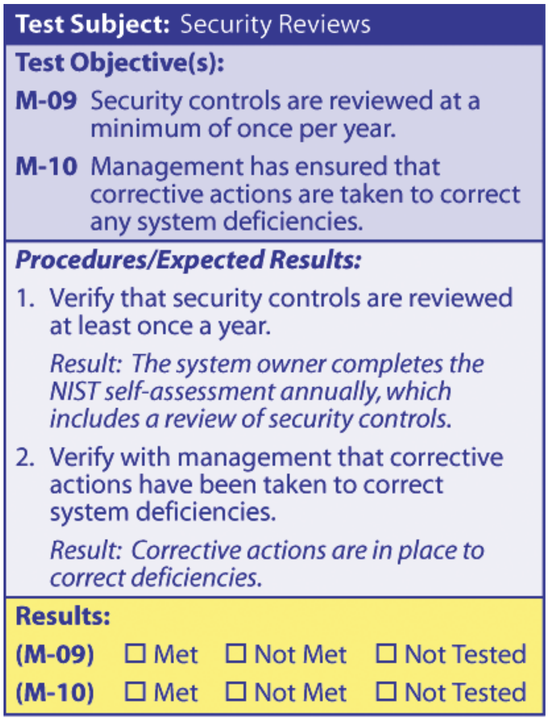
[3] See the *HHS Information Security Program Certification and Accreditation Guide* for a description of the security domain areas (management, operational, and technical) as they apply to the C&A process.

3.3 Step 3: Develop ST&E Procedures

Test procedures are used to validate the test objectives and verify that the system has met the stated test objective requirement.

The ST&E team develops initial ST&E procedures based on the test objectives. Procedures detail all steps, from start to finish, to verify the effectiveness of each security control implemented within the tier 3 or 4 GSS or MA being tested. Table 4 represents a suggested test procedure format.

Table 4. Test Procedure Format



Test Subject: Security Reviews

Test Objective(s):

M-09 Security controls are reviewed at a minimum of once per year.

M-10 Management has ensured that corrective actions are taken to correct any system deficiencies.

Procedures/Expected Results:

1. Verify that security controls are reviewed at least once a year.

   Result: The system owner completes the NIST self-assessment annually, which includes a review of security controls.

2. Verify with management that corrective actions have been taken to correct system deficiencies.

   Result: Corrective actions are in place to correct deficiencies.

Results:

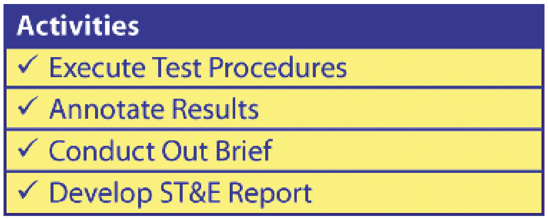
(M-09)	□ Met	□ Not Met	□ Not Tested
(M-10)	□ Met	□ Not Met	□ Not Tested

The ST&E team will perform a dry-run execution of the initial ST&E Plan. A dry run ensures that all test objectives, test procedures, and test scripts are accurate for the system being tested. The dry run cannot be performed until the test procedures are developed. The ST&E team may invite the system owner, ISSO, system and/or network administrators to participate in the dry-run test to assist with refining the ST&E Plan. If any of the information contained in the ST&E Plan is inaccurate, the ST&E team will correct the plan prior to formally executing it.

3.4 Step 4: Conduct ST&E and Document Results

Activities that the ST&E team will perform when conducting ST&E include (1) executing test procedures; (2) annotating met, not met, or not tested recording comments, or not met and not tested objectives; (3) conducting an informal out-brief; and (4) developing the draft ST&E Report. Table 5 identifies activities associated with conducting and documenting the results of an ST&E.

Table 5. Activities for Conducting ST&E and Documenting Results



Activities
✓ Execute Test Procedures
✓ Annotate Results
✓ Conduct Out Brief
✓ Develop ST&E Report

3.4.1 Execute Test Procedures

The ST&E team and the assigned system personnel will perform the test execution in accordance with the test procedures provided in the ST&E Plan. System administrators or other technical personnel should be present at the time of testing to witness and execute necessary test procedures. Multiple technical personnel may be required to execute the test. For example, a team member with training and experience in Windows NT system administration would be needed for Windows NT server testing, and a team member with Oracle database administration training and experience would be needed for database testing.

Prior to executing the ST&E Plan, the ST&E team should work with system personnel to ensure the following:

- Components scheduled for testing are operational.
- Required system personnel are available to assist with the ST&E process.

Depending on the type of test objective being tested, the ST&E team will perform or oversee the test and will gather results based on one or all of the following testing methods:

- **Observe** via hands-on execution, the system to verify security controls such as password complexity rules, warning banners, and password-protected screen savers.
- **Interview** system personnel (e.g., ISSO, system and network administrators) to identify information such as how passwords are distributed, how forgotten passwords are handled, and who is authorized to view audit logs.
- **Examine** system documentation such as rules of behavior, SSP, and contingency plans.

3.4.2 Annotate Results

It is critical that the ST&E team records whether each objective was “met”, “not met”, or “not tested.” This will enable the ST&E team to document comments for all failures, which will be identified as findings in the ST&E Report. Providing this information will allow the system owner to implement the necessary corrections, changes, or resolutions. Failure to meet the stated test objective could negatively impact system security and adversely affect the certification decision.

3.4.3 Conduct Out-Brief

After each component has been tested and corresponding results have been documented, an informal out-brief will take place between the ST&E team and the system owner. The out-brief is initiated to provide the system owner and other system personnel with descriptions of any findings (e.g., “not met” test objectives) resulting from the ST&E execution. Disclosure of the findings, especially any critical findings, provides the opportunity for immediate corrective action. Corrective actions can be implemented (and in some cases should be) before the report is finalized, and corrected findings should still be documented in the ST&E Reports.

Conducting the out-brief is an informal process because there may be items that need to be further examined at the conclusion of the ST&E. Once all necessary further examinations have been completed, the findings will be documented in the ST&E Report.

3.4.4 Develop ST&E Report

The ST&E team will develop an ST&E Report that includes results for each component tested, comments about additional information regarding the test objective, the test procedure and/or component tested, and findings (if applicable) for each test objective. The findings will be documented in a separate section of the report and will include:

- **Test objective**—the BLSR that was verified during the ST&E
- **Test objective number**—a unique number identifying the test objective
- **Finding description**—a description, including how and why, the test objective was not met during testing and what the actual results were when the test procedure(s) were executed
- **Control tested**—management, operational, or technical
- **Recommendation**—a description of how the finding may be corrected.

The system owner will receive a copy of the final ST&E Report and will be responsible for attaching the report, including any findings, as part of the system security documentation for the GSS or MA.

4. Summary

Executing an ST&E plays a critical role in the C&A process, ensuring that the security controls implemented in the GSS or MA have been tested and are compliant with HHS BLSRs. An ST&E assesses the technical and nontechnical implementation of a GSS or MA's security design to ascertain that security software, hardware, and firmware features affecting confidentiality, integrity, availability, and accountability have been properly implemented. This validates that the existing management, operational, and technical controls are properly implemented.

This guide provides information on implementing a structured ST&E approach for each of HHS' tier 3 and 4 GSSs or MAs. Specific questions or comments on the content of this guide should be directed to the HHS CSO.

Appendix A: Document Feedback Form

This form is for reviewer suggested corrections, revisions, or updates and is intended to improve the usefulness of the document for possible inclusion in future versions. Please forward recommended changes and comments to the U.S. Department of Health and Human Services (HHS), Office of the Chief Information Officer (OCIO).

By E-mail: <insert e-mail address>
Subject Line: Guidance Feedback
By Phone: <insert telephone number>

Document Title:

>

Section Number:

>

Category of Comment:

□	**A**	Administrative. Administrative comments correct what appear to be inconsistencies between sections, typographical errors, or grammatical errors.
□	**S**	Substantive. Substantive comments are provided because sections in the publication appear to be or are potentially incorrect, incomplete, misleading, or confusing.
□	**C**	Critical. Critical comments will cause non-concurrence with the publication if concerns are not satisfactorily resolved.
□	**M**	Major. Major comments are significant concerns that may result in a non-concurrence of the entire document if not satisfactorily resolved. This category may be used with a general statement of concern with a subject area, thrust of the document, etc., followed by detailed comments on specific entries in the publication which, taken together, constitute the concern.

Comment:

>

Name of Submitting Operating Division (OPDIV):

>

Your Name and Title:

>

Telephone:

>

E-mail:

>

Note: Use an additional blank sheet if needed.

Appendix B: References

HHS Information Technology Security Program Handbook, 2004.

HHS Information Technology Security Program Policy, 2005.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.

NIST SP 800-14*, Generally Accepted Principles and Practices for Securing Information Technology Systems,* September 1996.

NIST SP 800-16, Info*rmation Technology Security Training Requirements: A Role- and Performance-Based Model* (supersedes NIST SP 500-172),
April 1998.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*,
July 2002.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

NIST SP 800-42, *Guideline on Network Security Testing*, October 2003.

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources,* November 28, 2000.

OMB Circular A-130, *Management of Federal Information Resources,* Appendix III*, Security of Federal Automated Information Resources*, November 28, 2000.

Public Law 104-191, *Health Insurance Portability and Accountability Act of 1996* (HIPAA), August 21, 1996.

Public Law 107-347 [H.R. 2458], *The E-Government Act of 2002* —Title III of this Act is th*e Federal Information Security Management Act of 2002 (FISMA)*,
December 17, 2002.

Appendix C: Acronyms

BLSR	Baseline Security Requirements
CA	Certification Authority
C&A	Certification and Accreditation
CISO	Chief Information Security Officer
CMP	Configuration Management Plan
CSO	Chief Security Officer
DAA	Designated Approving Authority
DAC	Discretionary Access Controls
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act of 2002
GSS	General Support System
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IPSO	Information Processing Service Organization
ISA	Interconnection Security Agreement
ISSO	Information Systems Security Officer
IT	Information Technology
LAN	Local Area Network
MA	Major Application
MOA	Memorandum of Agreement
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPDIV	Operating Division
POA&M	Plan of Action and Milestones
PUB	Publication
SP	Special Publication
SSP	System Security Plan
ST&E	Security Test and Evaluation

Appendix D: Glossary

Accreditation—The formal declaration by the DAA that a major application or general support system is granted approval to process using a prescribed set of safeguards in a specific operational environment. The accreditation decision is made on the basis of a certification by designated technical personnel that the system meets prespecified technical requirements for achieving adequate security after the implementation of an agreed upon set of security controls. (See also: certification.) (Defined in NIST SP 800-18, Appendix D.)

Application—The use of information resources to satisfy a specific set of user requirements. (Defined in OMB Circular A-130, Appendix III, (A)(2)(b).)

Baseline Security Requirements (BLSR)—A set of obligatory standards, which serves as the basis for Management, Operational and Technical system security configuration, and by which system security controls are measured. Baseline Security Requirements can be modified only through a formal process of change control. See the *Handbook for Information Technology Security Risk Assessment Procedures* for more information.

Certification—A comprehensive analysis of the management, operational, and technical security controls in an information system, application, or network design, to establish the extent to which an implementation meets a set of pre-specified security requirements. This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the remaining vulnerabilities in the information system after the implementation of such controls. (See also: accreditation.) (Defined in NIST SP-37, Annex B.)

Discretionary Access Control (DAC)—Discretionary Access Control consists of something the user can manage, such as a document password. (Defined by SANS at http://www.sans.org/resources/glossary.php#A.)

General Support System (GSS)—An interconnected set of information resources under the same direct management control, which shares common functionality. A GSS normally includes hardware, software, information, data, applications, communications, and people. A GSS can be, for example, a local area network (LAN) including smart terminals that support a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO). (Defined in OMB Circular A-130, (A)(2)(c).)

Information System Security Officer (ISSO)—The principal staff advisor to the information system owner on all matters (technical and otherwise) involving the security of the information system. (Defined in DRAFT NIST 800-37, Annex B.)

Major Application (MA)—An application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function. (Defined in NIST SP 800-18) Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate. (Defined in OMB Circular A-130, (A)(2)(d).)

Penetration Testing—Involves attacks on or attempts to penetrate the security of a system for testing the effectiveness of the security and identifying any security vulnerabilities.

Risk—A measure of the degree to which information resources are exposed based on the probability that a threat will exploit vulnerability.

Risk Assessment—The process of analyzing threats to and vulnerabilities of an information system to determine its risks (potential for losses). The analysis forms the basis for identifying appropriate and cost-effective measures. See the *Handbook for Information Technology Security Risk Assessment Procedures* for more information.

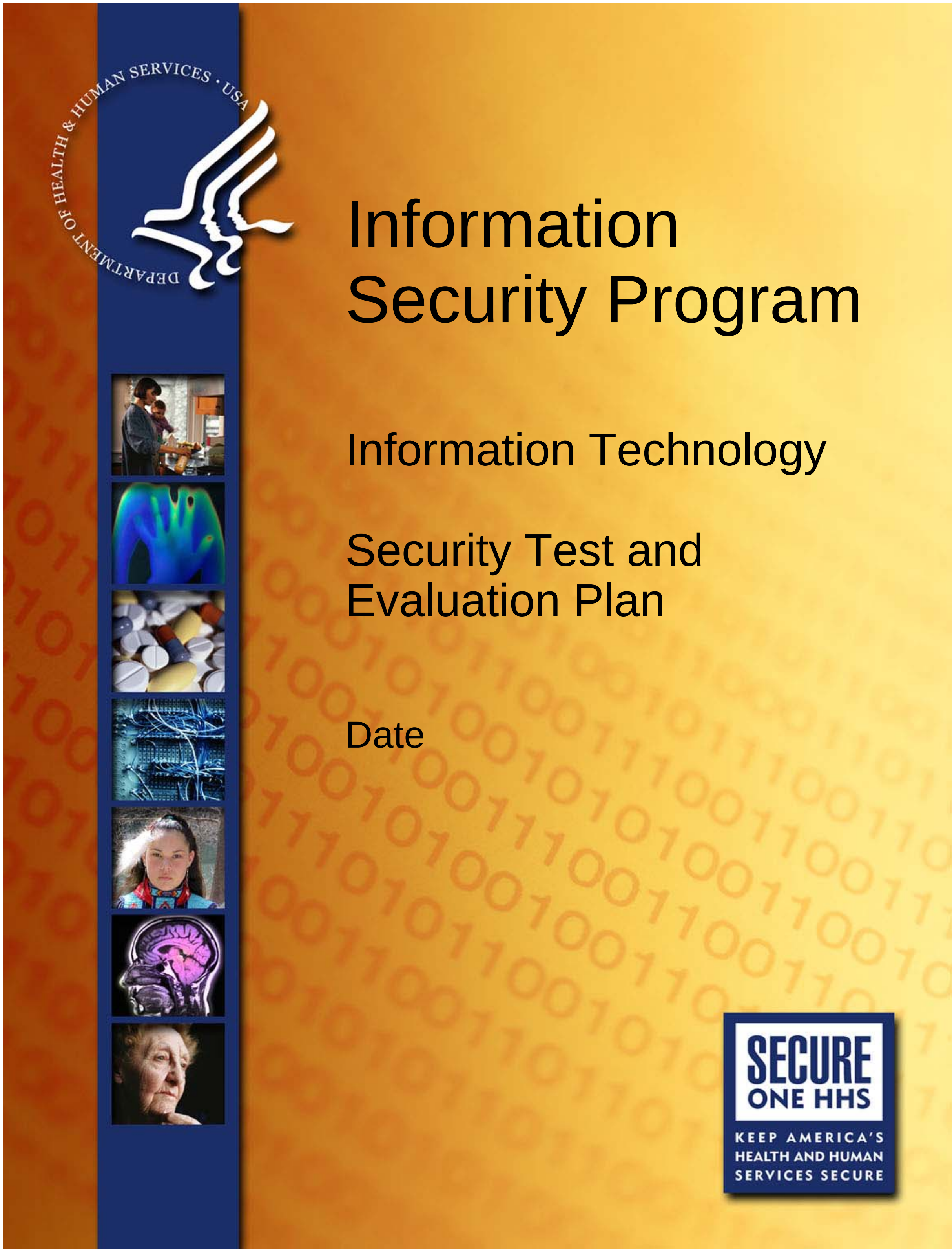
Risk Management—The process concerned with identification, measurement, controls, and minimization of security risk in information systems.

System Security Plan—A set of requirements that are used to delegate how system security will be managed. This plan includes system identification, management controls, operational controls, and technical controls. The system security plan outlines responsibilities for all system users and describes the rules of behavior for those users.

Threat—Any circumstance, event, or act that could cause harm by destroying, disclosing, modifying, or denying service to information resources.

Vulnerability—A condition that has the potential to be exploited by a threat. A weakness in an information system or component that could be exploited by a threat.

Appendix E: Security Test and Evaluation Plan Template



Information Security Program

Information Technology

Security Test and Evaluation Plan

Date

Table of Contents

1. Introduction

This document is the Security Test and Evaluation (ST&E) Plan for the Department of Health and Human Services (HHS) [insert system name]. Conducting an ST&E, in accordance with *HHS Information Security Program Certification and Accreditation Guide* and *Federal Information Security Management Act of 2002* (FISMA); the Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*; and the *Health Insurance Portability and Accountability Act of 1996* (HIPAA), is a critical step in the certification process required for HHS information systems.

1.1 Purpose

This ST&E Plan documents [insert agency name] approach to planning and conducting the [insert system name] ST&E activities required to support an accreditation decision. An ST&E involves planning and executing security tests and documenting the test results. The goals of the ST&E are to identify the security profile of the [insert system name] through hands-on testing in a controlled environment and to assess whether the system security configuration and controls meet the requirements for accreditation. The ST&E also verifies compliance with HHS baseline security requirements (BLSR) documented in *HHS Information Security Information Technology Risk Assessment Guide*. The ST&E results will be documented in an ST&E Report, which will serve as input to the [insert system name] accreditation decision.

1.2 Scope

This ST&E Plan identifies the security testing approach, the ST&E team, the resources required for ST&E execution, the execution process, and the schedule of primary activities. In addition, the plan addresses the system configuration at a high level, the components to be tested, and ST&E test objectives derived from the BLSRs. This plan includes step-by-step test procedures to be used in the verification of each test objective.

1.3 Background

[This section should include any pertinent information about the system. For example, it should include the purpose of the system, components, operational period, etc.]

Example:
The [insert system name] is a database management system used to track the various types of safety and wellness programs offered to the general public. The

system contains all the relevant programs, dates, contact names and numbers, and department responsible for leading the program.
The [insert system name] has been operational since 2001 and is maintained on server HHS123. Server HHS123 is running Windows 2000, Oracle 8i, and the [insert system name] application.

1.4 Document Overview

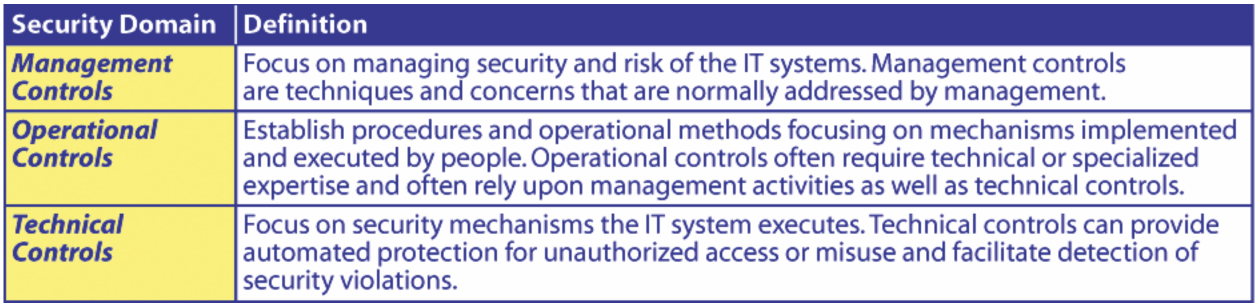
This document includes the following:

- Section 2 describes the ST&E methodology, evaluation criteria, test team composition, required resources, test execution, and test schedule.
- Section 3 describes security categories of test objectives.
- Appendix A contains a listing of acronyms used in this document.
- Appendix B provides specific system components' test procedures to be used.

2. Security Test and Evaluation Approach

This section outlines the ST&E approach, including ST&E methodology, evaluation criteria, test team composition, required resources, test execution, and test schedule. Through hands-on testing, interviews, and documentation review, the ST&E activities address security requirements of the [insert system name], the environment in which it is used, and operation regarding the security categories shown in Table 2-1. A primary goal is to verify the security posture of the system and identify findings as a result of the testing.

Table 2-1. Security Categories



Security Domain	Definition
Management Controls	Focus on managing security and risk of the IT systems. Management controls are techniques and concerns that are normally addressed by management.
Operational Controls	Establish procedures and operational methods focusing on mechanisms implemented and executed by people. Operational controls often require technical or specialized expertise and often rely upon management activities as well as technical controls.
Technical Controls	Focus on security mechanisms the IT system executes. Technical controls can provide automated protection for unauthorized access or misuse and facilitate detection of security violations.

2.1 ST&E Methodology

The ST&E methodology consists of a multistep approach. Figure 2-1 below presents the multistep approach that will be followed when performing the ST&E for [insert system name]. The figure represents the inputs, major activities, and outputs for each step involved in the ST&E methodology.

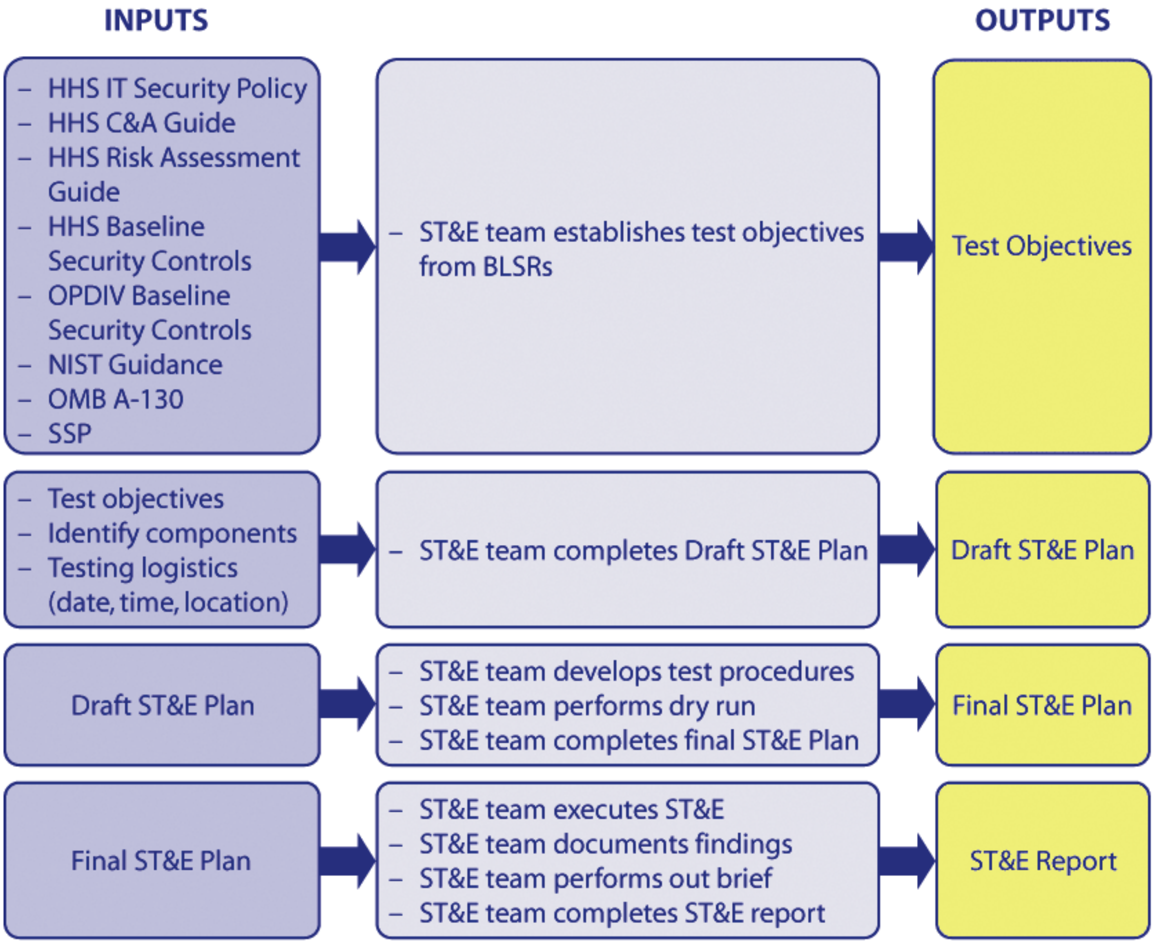

INPUTS
OUTPUTS
– HHS IT Security Policy
– HHS C&A Guide
– HHS Risk Assessment Guide
– HHS Baseline Security Controls
– OPDIV Baseline Security Controls
– NIST Guidance
– OMB A-130
– SSP
– ST&E team establishes test objectives from BLSRs
Test Objectives
– Test objectives
– Identify components
– Testing logistics (date, time, location)
– ST&E team completes Draft ST&E Plan
Draft ST&E Plan
Draft ST&E Plan
– ST&E team develops test procedures
– ST&E team performs dry run
– ST&E team completes final ST&E Plan
Final ST&E Plan
Final ST&E Plan
– ST&E team executes ST&E
– ST&E team documents findings
– ST&E team performs out brief
– ST&E team completes ST&E report
ST&E Report

Figure 2-1. [*insert system name*] ST&E Methodology

2.2 ST&E Evaluation Criteria

The results of each ST&E test procedure will be categorized into one of the following three ratings:

- **Met**—The stated test objective is met.
- **Not Met**—The stated test objective is not met.
- **Not Tested**—The test objective is not applicable at the time of testing.

All failures will be documented and included in the ST&E Report. Any test objective identified as not tested (N/T) to the [insert system name] means that the test objective is either not applicable or could not be tested because of a technical reason at the time of testing. Test objectives that are not tested will also be documented with associated comments in the ST&E Report.

2.3 ST&E Team

A [insert agency name] test team will be formed to support the ST&E activities. Test team responsibilities include planning, conducting, and documenting the results of the ST&E test process. HHS personnel will execute the test with [insert agency name] personnel witnessing the tests. HHS [insert system name] technical staff should be available to support the test execution activities as necessary.

The ST&E team's roles and responsibilities are defined as follows:

- **ST&E Test Engineer**—Conduct ST&E testing, record results, and support the verification process.
- **ST&E Test Witness**—Witness ST&E testing and verify results.
- **ST&E Support Engineer**—Troubleshoot equipment problems, and provide hardware and software expertise.

All ST&E team personnel are not required, on a daily basis, to be on site for testing. At a minimum, one ST&E test engineer and one ST&E test witness should be present during testing. Support personnel are not required to be on site during test execution, but must be available to report on site if required. ST&E activities, such as documentation review and system analysis, may be performed off site. Table 2-2 identifies expected personnel resources required of the participating groups or organizations.

Table 2-2. ST&E Staffing Requirements

Test Group	ST&E Test Engineer (conduct & monitor)	ST&E Test Witness	Support Engineer
[insert agency name] Test Team	1	1	
[insert system name] Technical Personnel		1	1
[Additional support groups should be listed here]			

2.4 ST&E Resources

This section identifies the resources required for ST&E test execution, including the necessary hardware, software, test accounts, and a preliminary list of documentation required for ST&E execution. Additional documentation may be requested during the execution of ST&E interviews.

2.4.1 Hardware/Software

[This section will include all hardware and software to be tested.]

All [insert system name] components are to be used operationally. Both the hardware and the software of these components should be configured for operational use throughout the duration of the ST&E. The ST&E process will be conducted in a controlled environment. Printer resources may be needed to print test result data, which will be used for analysis and archival of ST&E results. The following system components will be tested for [insert system name]:

Example:

- Windows 2000
- Oracle 8i
- [insert system name], version 1.1

2.4.2 Test Accounts

[This section will include a list of all accounts that will be used during the ST&E]

Example:
The following accounts will be used during the ST&E:

- System administrator account
- Database administrator account
- Application administrator
- System/test user accounts

2.5 Documentation

[List all applicable documentation that will be used to assist with conducting the ST&E.]

The following [insert system name] documentation, if available, may be required for ST&E activities:

- System Security Plan
- Configuration Management Plan
- Contingency Plan
- Risk Assessment Report
- Other related documents as needed

2.6 ST&E Execution

The following subsections address several aspects of the ST&E execution.

2.6.1 Assumptions and Constrains

The following assumptions and constraints apply to the ST&E execution:

- The ST&E team will have access to all HHS documentation as it pertains to the [insert system name] and its components.
- All application software, test software, and test data will be properly managed and controlled (e.g., diskettes and tapes).

2.6.2 Pre-ST&E Execution

If necessary, a “dry run” of ST&E procedures will occur to ensure the accuracy and validity of the steps. Test procedures will be refined throughout this process and the ST&E Plan will be updated accordingly.

Test objectives that may not be validated through hands-on testing may require information gathered through interviews or through documentation review. In this circumstance, the [insert agency name] test team will work with the [insert system name] system owner to schedule interviews with the appropriate system personnel and to gain access to specific documents.

2.6.3 ST&E Conduct

ST&E execution will follow the detailed step-by-step procedures as outlined in this plan. In circumstances where a general procedure has been defined, the system administrator will provide the [insert agency name] test team with detailed steps to execute during the test. Test procedure execution may not follow a particular sequence of order unless specifically stated by the system administrator. An ST&E test engineer will document the results of each test and will make note of anomalies. Certain test procedures may be required to be re-performed to confirm results. Operating system audit trail data will be printed for later review to verify that security-relevant test activities were properly captured (e.g., failed logins, failed file access).

2.6.4 Post ST&E Activities

The following activities will occur at the completion of test execution.

2.6.4.1 Prepare ST&E Report

The [insert agency name] test team will prepare an ST&E Report. This report will summarize security findings and address whether security weaknesses specified in the [insert system name] *Risk Assessment Report* have been resolved and/or mitigated. A thorough analysis of the security findings and the impact of unmet security requirements will be documented in the [insert system name] ST&E Report.

2.7 ST&E Schedule

This section presents the schedule for ST&E activities. The primary ST&E activities are as follows:

- **ST&E Plan**—A draft ST&E Plan will be delivered. Comments will be incorporated into a final ST&E Plan. The plan and procedures will be updated accordingly as the ST&E execution progresses.
- **ST&E Execution**—[This section would include an exact location or at a minimum the name of the facility, city, and state.]
- **ST&E Report**—The ST&E Report will be delivered no later than two weeks after completing the ST&E.

3. Security Test and Evaluation Objectives

The ST&E will provide an overall technical perspective of the security the [insert system name] affords while meeting its operational requirements. In addition, the successful demonstration that test objectives are satisfied provides the accrediting authority with a high level of assurance that system integrity and the integrity of the data stored within the [insert system name] cannot be compromised by internal or external sources.

The ST&E objectives seek to verify that the operational [insert system name] satisfies its BLSRs. Each test objective was derived from one or more BLSRs. Test objectives are organized into the following three security categories: (1) Management, (2) Operational, and (3) Technical controls. Test procedures were developed to verify that the objectives are categorized in the same way.

The first category of test objectives is Management Controls. The primary goal of the Management Control objectives is to verify the existence of documentation (e.g., system security plan, risk assessment) and to ensure that system responsibilities and roles are properly assigned. Test procedures developed to verify these objectives are nontechnical, including interviews, document reviews, and observations.

The second category of test objectives is Operational Controls. These test procedures were developed to ensure that operational controls and processes (e.g., incident response, contingency planning) are implemented effectively. Test procedures developed to verify these objectives are nontechnical, including interviews, document reviews, and observations.

The third category of test objectives is Technical Controls. These test procedures are technical and are customized for the component or operating system environment. In some cases all BLSRs will not apply to the individual component being tested. Technical test procedures require hands-on test execution.

Appendix A: Acronyms

BLSR	Baseline Security Requirements
DBA	Database Administrator
FISMA	Federal Information Security Management Act of 2002
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
N/T	Not Tested
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
ST&E	Security Test and Evaluation

Appendix B: Test Procedures

MANAGEMENT CONTROLS

Test Subject: Risk Assessment

Test Objective(s):

MC1.1: A risk assessment is performed and documented regularly (at least every three years, with self-assessments performed at least annually) or whenever the system, facility, or other conditions change. (BLSR RA-3)

MC1.2: The criticality and sensitivity levels of the IT system have been determined and documented. (BLSR RA-2)

MC1.3: An inventory exists for all critical-system software, applications, and computer and telecommunications hardware, including the system name and platform. (BLSR CM-2)

Procedures/*Expected Results*:

MC1.1:

1. Consult with the system owner to ensure that a risk assessment is performed and documented every three years or whenever a major change occurs.

   A risk assessment has been performed.

2. Consult with the system owner to ensure that a self-assessment is performed at least annually.

   A self-assessment has been performed at least annually.

MC1.2:

3. Determine if the criticality and sensitivity levels of the network have been determined and documented.

   The criticality and sensitivity levels have been determined and documented.

MC1.3:

4. Examine the inventory list for the system and determine if all software, applications, and computer and telecommunications hardware have been documented.

   The inventory list includes all sensitive applications and facilities for all software and hardware.

MC1.1	□ Met	□ Not Met	□ Not Tested
MC1.2	□ Met	□ Not Met	□ Not Tested
MC1.3	□ Met	□ Not Met	□ Not Tested

Comments:

Test Subject: Risk Assessment

Test Objective(s):

MC1.4: Based on the results of the risk assessments, remedial action plans [e.g., plan of action and milestone (POA&M), corrective action plan] have been developed and implemented to mitigate the impact of the threats identified. (BLSR IR-1, BLSR CA-5)

MC1.5: The extent of the risk assessment was commensurate with the complexity and cost of the system. (BLSR RA-3)

Procedures/*Expected Results*:

MC1.4:

1. Consult with management to determine if the results of the vulnerability assessments have been included in a remedial action plan to mitigate the impact of the threats identified.

   Management has developed a remedial action plan.

MC1.5:

2. Determine if a level of security has been established for this system that is commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the system.

   A level of security has been determined for the system.

MC1.4	□ **Met**	□ **Not Met**	□ **Not Tested**
MC1.5	□ **Met**	□ **Not Met**	□ **Not Tested**

Comments:

OPERATIONAL CONTROLS

Test Subject: Information Sharing and Interconnections

Test Objective(s):

OC1.1: Users are required to review a set of rules and regulations for system access prior to being granted system access. (BLSR PL-4)

OC1.2: Users sign an "acknowledgment statement" that they understand the system rules and regulations prior to being granted access. (BLSR PL-4)

Procedures/*Expected Results:*

OC1.1

1. Review the rules of behavior or equivalent set of rules for system access.

   The rules of behavior are obtained.

2. Verify that all users are required to read the set of rules of behavior prior to gaining system access.

   System users are required to read the rules of behavior prior to gaining system access.

OC1.2

3. Verify that users sign an acknowledge statement verifying that the rules of behavior have been read and agreed to.

   Users are required to sign an acknowledge statement.

OC1.1	□ **Met**	□ **Not Met**	□ **Not Tested**
OC1.2	□ **Met**	□ **Not Met**	□ **Not Tested**

Comments:

Test Subject: Security Awareness and Training

Test Objective(s):

OC1.3: The organization has a computer security training and awareness program. (BLSR AT-1)

OC1.4: The scope, goals, and objectives of the security awareness and training program have been documented. (BLSR AT-4)

OC1.5: All employees are provided security awareness training. (BLSR AT-2, BLSR AT-3)

Procedures/*Expected Results:*

OC1.3:

1. Verify that the organization has a computer-security training and awareness program.

    The organization has a computer-security training and awareness program.

OC1.4:

2. Verify that the training program has a documented scope, goals, and objectives.

    The training program has a documented scope, goals, and objectives.

OC1.5:

3. Verify that all employees are provided security and awareness training.

    All employees are provided security and awareness training.

OC1.3	□ **Met**	□ **Not Met**	□ **Not Tested**
OC1.4	□ **Met**	□ **Not Met**	□ **Not Tested**
OC1.5	□ **Met**	□ **Not Met**	□ **Not Tested**

Comments:

TECHNICAL CONTROLS

Test Subject: Logical Access Control

Test Objective(s):

TC1.1: A warning message (log-on banner) is displayed, notifying unauthorized users that they have accessed a U.S. Government computer system.* (BLSR AC-8)

Procedures/*Expected Results:*

1. Go to Start | Run, type regedt32 and press <Enter>. When the Registry Editor appears, go to the following registry keys: HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon

   The "LegalNoticeCaption" and "LegalNoticeText" keys provide the required HHS banner security warning.

*This test applies to Windows 2000.

TC1.1	□ **Met**	□ **Not Met**	□ **Not Tested**

Comments:

Test Subject: Identification and Authentication

Test Objective(s):

TC1.2: Passwords are changed every 120 days.* (BLSR IA-5)

Procedures/*Expected Results*:

1. As database administrator (DBA), type the following command to display the value of password life time:

```
select *
from DBA_PROFILES
where RESOURCE_NAME= ‘PASSWORD_LIFE_TIME’;
```

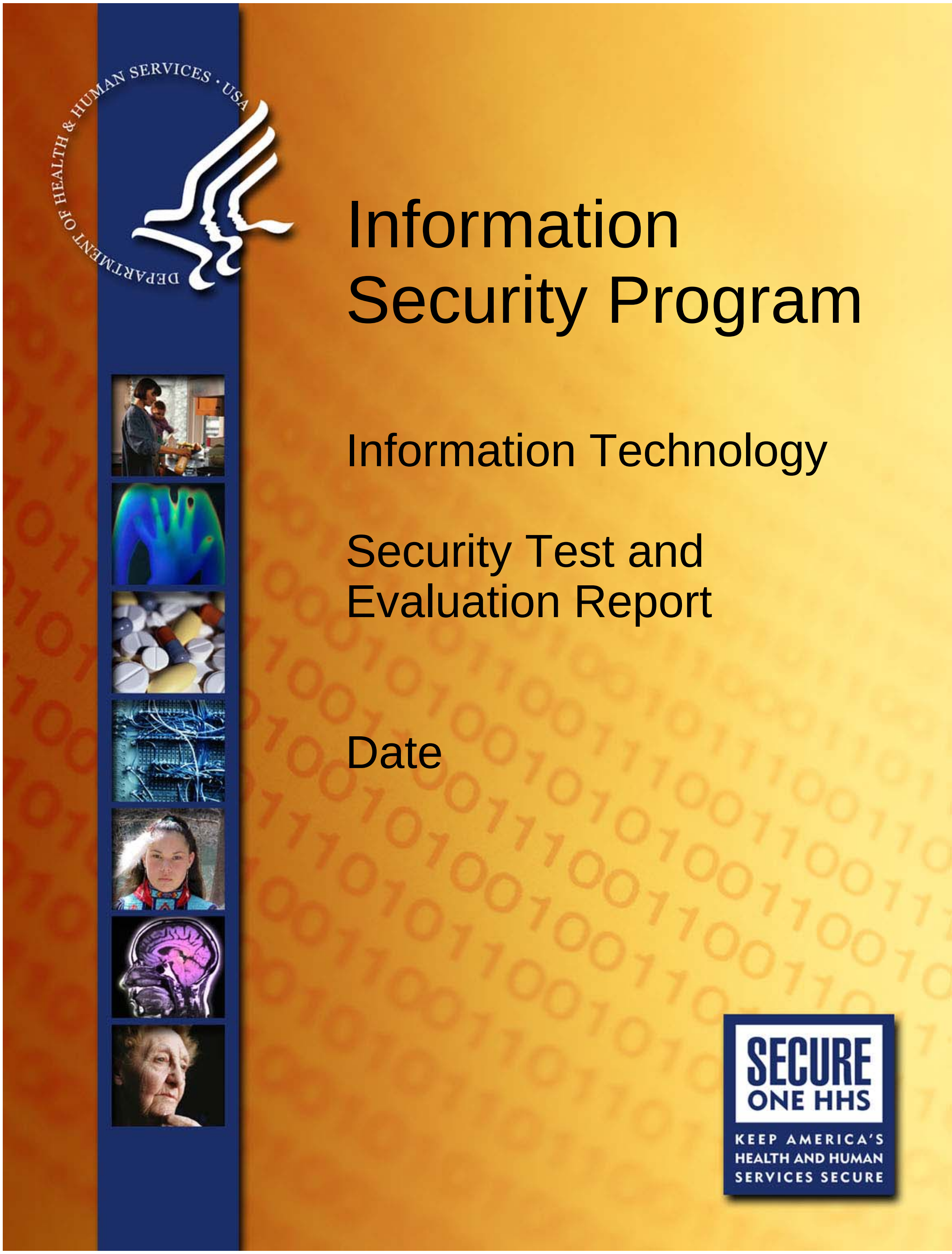
PASSWORD_LIFE_TIME is set to 120.

*This test applies to Oracle 8i.

TC1.2 □ **Met** □ **Not Met** □ **Not Tested**

Comments:

Appendix F: Security Test and Evaluation Report Template



Information Security Program

Information Technology

Security Test and Evaluation Report

Date

Table of Contents

Executive Summary

[insert agency name] performed a Security Test and Evaluation (ST&E) for the [insert agency name] [insert system name] on [insert date]. The tests were performed at the [insert location of where testing occurred].

The ST&E execution followed the methodology, test objectives, and detailed procedures described in the [insert document name] dated [insert date]. The purpose of conducting the ST&E was to identify vulnerabilities of [insert system name] through hands-on testing in a controlled environment and to assess whether the system configuration and controls met requirements for accreditation. The ST&E consisted of management, operational, and technical test objectives and procedures for the following components:

[insert list of components]

Example:

A total of [insert number of findings] were identified for [insert system name]; [insert number of findings] were identified resulting from the ST&E.

[insert all findings in the table below.]

Table ES-1. [insert system name] Summary of Findings

Finding Number	Description	Test Objectives	Risk Level
Management Controls			
1	Self-assessments are not performed annually.	MC1.1	Medium
2	Plan of action and milestones (POA&M) and corrective action plans have not been developed as a result of the security assessments performed.	MC1.4	Medium
Operational Controls			
1	Users do not sign an acknowledgement statement indicating that they have read the rules of behavior.	OC1.2	Medium
2	Contractors do not participate in security awareness training.	OC1.5	Medium
Technical Controls			
1	A warning message is not displayed on the Windows 2000 operating system prior to accessing the system.	TC1.1	High

1. Introduction

[insert agency name] performed a security test and evaluation (ST&E) for the [insert agency name] [insert system name] on [insert date] located in [insert location of where testing occurred]. The ST&E execution followed the methodology, test objectives, and detailed procedures described in the [insert document name] dated [insert date].

1.1 Purpose

This report documents the test results of the ST&E and provides an evaluation and analysis of the test objectives considered “not met.” The ST&E was conducted to identify the security provided by [insert system name] through hands-on testing in a controlled environment and to assess whether the system configuration and controls meet the requirements of [insert agency name].

1.2 Scope

The ST&E test was conducted against the [insert system name] system components housed in the [insert name of facility where the system is housed]. However, the [insert components that were not tested (e.g., DHS Rack Pack and Load Balancer)] were not included for the ST&E. This report documents only the test results as identified during the testing*.* A detailed analysis of each finding related to threats to and vulnerabilities of [insert system name] and associated risks will be documented in the [insert system name] *Risk Assessment Report*. The test procedures contained in the [insert system name] *ST&E Plan* have been revised to reflect changes made during the test execution and are provided in appendices with the completed test procedure worksheets.

1.3 Document Overview

This document is organized in four sections. This section provides a general introduction. Section 2 provides a description of the test system configuration. Section 3 documents test results, including the detailed findings for the test objectives that were identified as “not met” or failed. Appendix A is an acronym list. Appendix B contains the ST&E worksheet with the results of each test. The result for each test objective is documented at the end of the test procedure worksheet. These results are presented by “met”, “not met”, or “not tested” for each [insert system name] test objective.

2. Test System Configuration

2.1 System Description

[Provide a brief description of the system.]

2.2 System Components

[Describe the components tested.]

2.3 ST&E Execution

The ST&E consisted of management, operational, and technical controls. The ST&E objectives were developed to verify whether the operational [insert system name] satisfies its baseline security requirements (BLSR). Each test objective was derived from one or more BLSRs. Technical controls were tested on the following system components:

Example:

- Windows 2000
- Oracle 8i
- [insert system name], version 1.1

2.4 Test Team

[Describe the test team to include the contractor personnel and HHS personnel present at the time of testing.]

Example:
The test team consisted of two [insert agency name] personnel and the three HHS system administrators. The primary responsibility of the test team was to conduct and document the results of the ST&E process. The ST&E was performed with the assistance of the application administrator and system administrators. The components were tested from the administrators’ workstations and at the console located in the HHS.

3. Test Results

This section documents the test objectives that have been identified as “not met” or failed as results of the ST&E performed against the [insert system name] components. The findings statements for management and operational controls are listed accordingly, while the technical control findings are listed by component. Related or similar findings were grouped for discussion purposes.

3.1 Management Controls

Two findings were associated with the management control section.

[Document all findings as a result of the ST&E. See the examples below.]

Finding 1: Self-assessments are not performed annually.

Self-assessments have not been performed for the [insert system]. System owners and managers do not have a method of tracking system inventory, information sensitivity, and system criticality levels.

Test Objective(s): MC1.1 Risk Level: [insert risk level]
Example: Medium

Recommendation: Perform self-assessments for [insert system] annually and in accordance with the National Institute of Standards and Technology (NIST) 800-26.

Finding 2: Plan of action and milestones (POA&M) and corrective action plans have not been developed as a result of the security assessments performed.

Management has not developed a formal POA&M or corrective action plan for the system. The vulnerabilities and risks identified in the risk assessment have not been included in a plan to facilitate corrective actions. A POA&M is required by NIST 800-37 and must be included in the certification and accreditation package.

Test Objective(s): MC1.4 Risk Level: [insert risk level]
Example: Medium

Recommendation: Develop a POA&M to include the results of any security assessments performed on the system (e.g., risk assessment, ST&E).

3.2 Operational Controls

Two findings were associated with the operational control section.

[Document all findings as a result of the ST&E. See the examples below.]

Finding 1: Users do not sign an acknowledgement statement indicating that they have read the rules of behavior.

Although rules of behavior exist for the system, there is no acknowledgement statement or signature form that states that users read, understood, and agreed to the rules.

Test Objective (s): OC1.2 Risk Level: [insert risk level]
Example: Medium

Recommendation: Create a signature page at the end of the rules of behavior document. Require that all users sign this form prior to being granted system access.

Finding 2: Contractors do not participate in security awareness training.

HHS has a standard security awareness training program; however, contractors are not required to attend. The security awareness training program requires that all employees upon hire must attend the training courses provided during that hiring period.

Test Objective (s): OC1.5 Risk Level:[insert risk level]
Example: Medium

Recommendation: Require that contractors attend the security awareness training programs required for all HHS employees.

3.3 Technical Controls

One finding was associated with the technical control section.

[Document all findings as a result of the ST&E. See the example below.]

Finding 1: A warning message is not displayed on the Windows 2000 operating system prior to accessing the system.

A warning banner (log-on banner) must be displayed at all access points on the system notifying unauthorized users that they have accessed a U.S. Government computer system. This would apply to the Windows 2000 operating system, Oracle 8i, and the [insert system name]. The Windows 2000 operating system does not meet this requirement.

Test Objective (s): TC1.1 Risk Level:[insert risk level]
Example: High

Recommendation: Configure the “LegalNoticeCaption” and “LegalNoticeText” options in the following registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\ WindowsNT\CurrentVersion\Winlogon in regedt32 with the standard HHS warning message.

Appendix A: Acronym List

BLSR	Baseline Security Requirements
DBA	Database Administrator
IT	Information Technology
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
ST&E	Security Test and Evaluation

Appendix B: Test Procedures

MANAGEMENT CONTROLS

Test Subject: Risk Assessment

Test Objective(s):

MC1.1: A risk assessment is performed and documented regularly (at least every three years, with self-assessments performed at least annually) or whenever the system, facility, or other conditions change. (BLSR RA-3)

MC1.2: The criticality and sensitivity levels of the information technology (IT) system have been determined and documented. (BLSR RA-2)

MC1.3: An inventory exists for all critical-system software, applications, and computer and telecommunications hardware, including the system name and platform. (BLSR CM-2)

Procedures/*Expected Results*:

MC1.1:

1. Consult with the system owner to ensure that a risk assessment is performed and documented every three years or whenever a major change occurs.

   A risk assessment has been performed.

2. Consult with the system owner to ensure that a self-assessment is performed at least annually.

   A self-assessment has been performed at least annually.

MC1.2:

3. Determine if the criticality and sensitivity levels of the network have been determined and documented.

   The criticality and sensitivity levels have been determined and documented.

MC1.3:

4. Examine the inventory list for the system and determine if all software, applications, and computer and telecommunications hardware have been documented.

   The inventory list includes all sensitive applications and facilities for all software and hardware.

MC1.1	□ **Met**	☑ **Not Met**	□ **Not Tested**
MC1.2	☑ **Met**	□ **Not Met**	□ **Not Tested**
MC1.3	☑ **Met**	□ **Not Met**	□ **Not Tested**

Comments:

Test Subject: Risk Assessment

Test Objective(s):

MC1.4: Based on the results of the risk assessments, remedial action plans [e.g., plan of action and milestone (POA&M), corrective action plan] have been developed and implemented to mitigate the impact of the threats identified. (BLSR IR-1, BLSR CA-5)

MC1.5: The extent of the risk assessment was commensurate with the complexity and cost of the system. (BLSR RA-3)

Procedures/*Expected Results*:

MC1.4:

1. Consult with management to determine if the results of the vulnerability assessments have been included in a remedial action plan to mitigate the impact of the threats identified.

   Management has developed a remedial action plan.

MC1.5:

2. Determine if a level of security has been established for this system that is commensurate with the sensitivity of the information and the risk and magnitude of loss or harm that could result from improper operation of the system.

   A level of security has been determined for the system.

MC1.4	□ **Met**	☑ **Not Met**	□ **Not Tested**
MC1.5	☑ **Met**	□ **Not Met**	□ **Not Tested**

Comments:

OPERATIONAL CONTROLS

Test Subject: Information Sharing and Interconnections

Test Objective(s):

OC1.1: Users are required to review a set of rules and regulations for system access prior to being granted system access. (BLSR PL-4)

OC1.2: Users sign an acknowledgment statement that they understand the system rules and regulations prior to being granted access. (BLSR PL-4)

Procedures/*Expected Results:*

OC1.1

1. Review the rules of behavior or equivalent set of rules for system access.

   The rules of behavior are obtained.

2. Verify that all users are required to read the set of rules of behavior prior to gaining system access.

   System users are required to read the rules of behavior prior to gaining system access.

OC1.2

3. Verify that users sign an acknowledge statement verifying that the rules of behavior have been read and agreed to.

   Users are required to sign an acknowledge statement.

OC1.1	☑ **Met**	□ **Not Met**	□ **Not Tested**
OC1.2	□ **Met**	☑ **Not Met**	□ **Not Tested**

Comments:

Test Subject: Security Awareness and Training

Test Objective(s):

OC1.3: The organization has a computer-security training and awareness program. (BLSR AT-1)
OC1.4: The scope, goals, and objectives of the security awareness and training program have been documented. (BLSR AT-4)
OC1.5: All employees are provided security awareness training. (BLSR AT-2, BLSR AT-3)

Procedures/*Expected Results:*

OC1.3:

1. Verify that the organization has a computer-security training and awareness program.

   The organization has a computer-security training and awareness program.

OC1.4:

2. Verify that the training program has documented scope, goals, and objectives.

   The training program has documented scope, goals, and objectives.

OC1.5:

3. Verify that all employees are provided security and awareness training.

   All employees are provided security and awareness training.

OC1.3	☑ **Met**	□ **Not Met**	□ **Not Tested**
OC1.4	☑ **Met**	□ **Not Met**	□ **Not Tested**
OC1.5	□ **Met**	☑ **Not Met**	□ **Not Tested**

Comments:

TECHNICAL CONTROLS

Test Subject: Logical Access Control

Test Objective(s):

TC1.1: A warning message (log-on banner) is displayed, notifying unauthorized users that they have accessed a U.S. Government computer system.* (BLSR AC-8)

Procedures/*Expected Results:*

1. Go to Start | Run, type regedt32 and press <Enter>. When the Registry Editor appears, go to the following registry keys:
HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\
Winlogon

   The "LegalNoticeCaption" and "LegalNoticeText" keys provide the required HHS banner security warning.

*This test applies to Windows 2000.

TC1.1	□ **Met**	☑ **Not Met**	□ **Not Tested**

Comments:

Test Subject: Identification and Authentication

Test Objective(s):

TC1.2: Change passwords every 120 days.* (BLSR IA-5)

Procedures/*Expected Results*:

1. As DBA, type the following command to display the value of password life time:

```
select *
from DBA_PROFILES
where RESOURCE_NAME= ‘PASSWORD_LIFE_TIME’;
```

PASSWORD_LIFE_TIME is set to 120.

*This test applies to Oracle 8i.

TC1.2 ☑ **Met** □ **Not Met** □ **Not Tested**

Comments:

Appendix G: Information Security Program Documents

The Department of Health and Human Service (HHS) Information Technology Security Program is supplemented by a series of HHS Information Security documents. These documents include:

- HHS Information Security Program Policy
- HHS Information Security Program Handbook
- HHS Information Security Program Rules of Behavior
- Baseline Security Requirements Guide
- Certification and Accreditation (C&A) Guide
- Configuration Management Guide
- Contingency Planning for Information Security Systems Guide
- Critical Infrastructure Protection (CIP) Planning Guide
- Data Cryptography Guide
- Disaster Recovery Planning Guide
- Firewall Configuration Guide
- Health Insurance Portability and Accountability Act (HIPAA) Compliance Guide
- Incident Response Planning Guide
- Information Privacy Program Policy
- Information Privacy Program Handbook
- Information Technology (IT) Penetration Testing Guide
- IT Personnel Security Guide
- IT Physical and Environmental Security Guide
- IT Privacy Impact Assessment Guide
- IT Security Capital Planning Guide
- Machine-Readable Privacy Policy Guide
- Plan of Actions and Milestones (POA&M) Guide
- Risk Assessment Guide
- Security Test and Evaluation (ST&E) Planning Guide
- Web Security Guide
- Wireless Security Program Development Guide

Acknowledgements

Carlos Figueroa and Joanna Ganiear were instrumental in developing this document.