[Insert System Name/Acronym]

Security Test and Evaluation (ST&E) Plan

Version *[Insert #]*

[Insert Date]

Prepared by

[Insert Group/Organization/Company Name]
[Insert Street Address]
[Insert City, State, and Zip Code]

Document Change Control

Version	Release Date	Summary of Changes	Addendum Number[1]	Name
Version *[0.1]*	*[Insert Date]*	*[Insert Summary of Changes]*	*[Insert Addendum #]*	*[Insert Name]*

[1] Minor changes should be recorded in the addendum section of this document. These changes must be incorporated into the main document upon the next full document release (at least annually).

TABLE OF CONTENTS

[This sample format provides a template for preparing an System ST&E Plan . The template is intended to be used as a guide, and the preparer should modify the format as necessary to document the plan for testing the system security controls to ensure compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53.

Where practical, the template provides instructions [in bold blue text] for completing specific sections. Delete template text after the plan has been populated with specific system information.

1. INTRODUCTION

1.1 Purpose

The purpose of this document is to establish and define the plan for the ***[Insert System Name/Acronym]*** Security Test and Evaluation (ST&E). The ST&E Plan provides; (i) the security testing approach, (ii) the ST&E execution team, (iii) the resources required for test execution, (iv) the execution process, and (v) the schedule of primary activities. In addition, this Plan describes the system at a high level, the system modules to be tested, and the step-by-step test cases used to verify the implementation of each security control.[1]

1.2 Background

ST&E is an analysis of the non-technical and technical security controls required to protect information and information systems, that have been implemented in an operational environment. The ST&E determines the extent to which a set of specified security requirements are met. This document is the plan for verifying the correct implementation of the NIST SP 800-53 controls identified and documented in the System Security Plan (SSP) for ***[Insert System Acronym]*** in support of the certification and accreditation (C&A) process. In addition, the ST&E plan verifies that ***[Insert Organization]*** security standards are met. The ST&E results will be used to identify and document the risks of the system in the Security Assessment Report (SAR).

1.3 Scope

The ST&E will address the ***[Insert Organization]***'s confidentiality, integrity, and availability requirements that provide the necessary protections for the ***[Insert System Acronym]*** identified within the system's boundary.

[Add system description and other relevant background information that defines the scope of the ST&E to include the testing site or sites once agreed upon.]

1.4 Assumptions and Constraints

The following assumptions and constraints were taken into consideration when developing this ST&E Plan:

- The ST&E process will be conducted in a controlled development/test environment.
- The ST&E Execution team will have access to all relevant documentation for the system.
- All system media will be properly managed and controlled (e.g., diskettes and Optical devices) in accordance with ***[Insert Organization Policy]***.
- Both the hardware and software is configured for operational use throughout the duration of the testing.
- ***[Insert system specific assumptions and constraints, if any.]***

[1] The vulnerabilities identified during testing will be documented in the ST&E Findings Matrix and will be used in developing the SAR.

1.5 ST&E Execution Team Roles and Responsibilities

The ST&E Execution Team is responsible for planning, executing, and documenting the results of the ST&E. Table 1 provides a list of the team members, including their role(s) and a short description of their responsibilities.

Table 1. ST&E Execution Team

Name	Organization	Role	Responsibility
		ST&E Execution Team Lead	Coordinate and execute ST&E, record/verify results.
		ST&E Test Engineer	Execute ST&E, record/verify results.
		ST&E Test Witness	Witness testing and verify results.
		System POC(s)	All key stroke testing of the system will be performed by the designated System POC(s).
		Support Engineer	Troubleshoot equipment problems, as necessary, and provide hardware and software expertise.
		[Add additional roles as appropriate]	

At a minimum, one ST&E Test Engineer and one ST&E Test Witness will be present during testing. Support personnel are not required to be on-site during test execution; however, they must be available to report on-site if required.

For test cases where login to the system is required, the ST&E Test Engineer role will be assigned to an ***[Insert Organization]*** or ***[Insert Organization]***-designated individual, who has access to the system.

1.6 Organization

The remainder of this document is organized as follows:

- Section 2 provides the ST&E approach
- Section 3 describes the ST&E schedule
- Appendix A contains the acronym list
- Appendix B contains the ST&E Test Plan Matrix to be used for the ST&E

2. ST&E APPROACH

2.1 Develop Test Plan

The ST&E Test Plan is populated with the step-by-step cases for testing the applicable NIST SP 800-53 security controls as described in the SSP. In addition, during the ST&E execution process, the ST&E Test Plan is populated with the results of the testing for each security control tested. This following sections describe the format/content of the ST&E Test Plan and also discusses sample sizes and utilization of existing test results.

2.1.1. Format and Content

The ST&E Test Plan Matrix or Security Requirements Traceability Matrix (SRTM) contains:

- NIST SP 800-53 Control type
- NIST SP 800-53 Control number
- NIST SP 800-53 Case number
- NIST SP 800-53 Control technology
- Sample Size
- Test Case(s) (the specific step-by-step procedures for testing the security control)
- Expected result(s) (contains the expected results of the execution of the test cases)
- Interviewee (Point of contact responsible for answering test cases)
- Actual result(s) (contains the actual results received from the execution of the test cases)
- Pass/Fail
- Comments (contains the ST&E Execution Team specific comments that pertain to the security control)
- Collected evidence for each control
- Tester for each control

2.1.2. Sample Size(s)

During execution, the ST&E Execution Team frequently does not examine all of the information available as it may be impractical and valid conclusions can be reached using sampling. The specific sample size will be documented in the ST&E test cases, as appropriate.

2.1.3. Existing Test Results

In the instance where test cases have been previously executed and the results documented, the ST&E Execution Team will review the existing test cases and test results to determine if the documented results are reliable[3]. If reliable, the documented results will be leveraged for the current ST&E. Furthermore, limited or no additional testing may be required for the controls tested under a previous reliable test.

As such, in the instance, where security controls have previously been tested as part of another system ST&E, the results will be leveraged across all other system ST&Es as applicable (e.g., in

[3] *Reliable* results should at least meet the following criterion: (i) no significant changes should have occurred that directly or indirectly effect the test cases, and (ii) the previous execution should have been performed within the last three (3) years.

the case, where multiple systems reside on the same database and the database has previously been tested as part of another system ST&E the results will be leverage across all of the system ST&Es that reside on that same database).

2.2 Execute ST&E

The ST&E Execution Team will work with the designated System Point of Contact(s) (POC) to execute the test cases in accordance with this Plan. All key stroke testing of the system will be performed by the designated System POC(s). The ST&E Execution Team will document the actual results and any comments regarding each test as necessary. In order to support the results of each test, the ST&E Execution Team will reference the applicable documentation. The following paragraph provides a description of the test cases.

2.2.1. Test Cases

The NIST SP 800-53 security controls (managerial, operational, and technical) are verified to ensure conformity to ***[Insert Organization]*** configuration requirements and are developed as test cases in this document. The test cases provide the steps for examining each critical component of the system, and define how each security control is implemented.

The test cases specify the actions required to perform the test on each component, and are implemented by a manual checklist or automated tool. The ST&E Test Plan matrix contains the set of test cases used to conduct the ST&E. Some test cases are non-technical in nature, and will require information gathered through interviews or documentation examination instead of hands-on technical testing.

In cases where the actual results do not match the expected results of a test case, the ST&E Execution Team will inquire about existing exceptions for that control. Exceptions not already collected by the C&A Team, will be collected by the ST&E Execution Team.

2.2.2. Supporting Evidence

Indirect or direct information obtained to support the implementation of a specific security control will be documented and retained as supporting evidence.

2.2.3. Inherited Security Controls

The *inherited security controls*, as defined in NIST SP 800-53 and determined during the SSP development, that are provided by the General Support System (CC-GSS) that the system resides on and will not be tested as part of the system ST&E. Instead, the GSS ST&E will be referenced. In addition, inherited security controls across the ***[Insert Organization]*** (CC-ORG) will be tested once across the organization and the test results will be utilized for all system ST&E results, as appropriate.

2.2.4. Testing Environment

ST&E execution will take place in the system/GSS production environment. If this is not possible, it is the responsibility of the ST&E Execution Team to determine if the development/test environment mirrors the production environment. In the instance where the development/test environment does *not* mirror the production environment, the ST&E Execution

Team will confer with the system POCs and C&A stakeholders to determine the best course of action to execute the test cases.

Include the testing site or sites once agreed upon in the paragraph above.

2.3 Document Test Results

The ST&E Execution Team is responsible for documenting the results of the test cases in the ST&E Test Plan and the ST&E Findings Matrix. The ST&E Execution Team will provide the completed ST&E Test Plan and ST&E Findings Matrix to the C&A Team for a quality control review. The C&A Team will review the matrix and provide comments to the ST&E Execution Team as necessary. The ST&E Execution Team will revise the matrices, addressing the C&A Team's comments. All supporting documentation providing evidence for the ST&E results will be submitted to the Risk Assessment Team. Prior to submission, the ST&E Execution Team will convert all hard copy supporting documentation into electronic format (i.e., Adobe Acrobat PDF).

3. SCHEDULE

Activity/Deliverable	Start Date	End Date

APPENDIX A. ACRONYMS

[Add the system acronym to this list, as well as any acronyms used within the "background" section of the ST&E Plan.]

C&A	Certification and Accreditation
DBA	Database Administrator
FIPS PUB	Federal Information Processing Standards Publication
GSS	General Support System
I&A	Identification and Authentication
IA	Information Assurance
NIST	National Institute of Standards and Technology
PDF	Portable Document Format
POC	Points of Contact
SA	System Administrator
SAR	Security Assessment Report
SP	Special Publication
SSP	System Security Plan
ST&E	Security Test and Evaluation

APPENDIX B. ST&E PLAN MATRIX

Please refer to the ***[Insert Application Acronym]*** ST&E Plan Matrix or Security Requirements Traceability Matrix (SRTM).