Security Test and Evaluation (ST&E)

<Company Name>

<Company Logo>

<System Name>

<Date>

Table of Contents

1. Introduction

This document provides guidance on the Security Test and Evaluation (ST&E) process. ST&E activities are an essential component of the Accreditation and Authorization (A&A) process. The purpose of ST&E is to determine the Information Technology (IT) system's compliance with the security requirements documented in the security plan and to verify that the minimal security controls identified in the plan are correctly implemented and effective.

The ST&E is conducted on new or upgraded systems (after delivery and installation) during the test phase of the lifecycle or on legacy systems during the operation/maintenance phase of the lifecycle.

ST&E reports typically contain the results of testing and evaluation conducted on the IT system at the site where the system is deployed for operation to verify that the technical, management, and operational security controls are implemented correctly. ST&E may include interviews with personnel responsible for the security or operation of the system, review of documentation which defines expected policies and protocols to be enforced, demonstrations or review of artifacts that are produced during routine operation of the system, and environment and functional testing of the technical controls that are applied.

The use of standardized verification techniques and procedures supports consistent, analogous, and repeatable security certifications of IT systems and an efficient and cost-effective A&A process.

1.1 Overview

The ST&E process is designed to gain objective evidence of proper implementation and functionality of an IT system's security features. The activities identified in this ST&E guide are applicable to all IT systems.

The successful completion of ST&E activities provides the Authorizing Official (AO) with a high level of assurance that the IT system satisfies the Federal requirements for Controlled Unclassified Information (CUI) IT systems.

The objectives of the ST&E process are to:

- Uncover design, implementation, and operational flaws that could be used to exploit IT resources.
- Verify that appropriate security mechanisms, assurances, and other properties have been implemented to enforce the security policy.
- Determine the adequacy of those security mechanisms, assurances, and other properties to enforce the security policy.
- Assess the degree of consistency between the IT system documentation and its implementation.