MTR 02W0000059

MITRE TECHNICAL REPORT

FAA System Security Testing and Evaluation

May 2003

Marshall D. Abrams

Sponsor: Federal Aviation Administration **Contract No.:** DTFA01-01-C-00001
Dept. No.: F083 **Project No.:** 02033312-IG

MITRE
Center for Advanced Aviation System Development
McLean, Virginia

MITRE Department Approval:

Gary D. Forman

Associate Program Manager

MITRE Project Approval:

Duncan Thomson

Outcome Leader

Abstract

Security requirements and security testing of an Federal Aviation Administration (FAA) System are described for systems during planning, development, and operation. The guidance herein for security testing and evaluation follows best practice in security testing, exemplified by the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) based on the *Common Evaluation Methodology* (CEM) for developmental systems and the National Institute of Standards and Technology (NIST) *Guideline on Network Security Testing* for operational systems.

Security testing is part of the analysis of security properties in developmental systems. These security properties are verified relative to the functional specification, guidance documentation, and the high-level design of the system. The analysis is supported by independent testing of a subset of the system security functions, evidence of developer testing based on the functional specification, dynamically selective confirmation of the developer test results, analysis of strength of functions, and evidence of a developer search for obvious vulnerabilities. Some testing of installed operational systems repeats the tests performed on the developmental systems, while other testing is unique to the operational in-service phase.

Operational system security testing should be integrated into an organization's security program. The primary reason for testing an operational system is to identify potential vulnerabilities and repair them prior to going operational. The following types of testing are described: network mapping, vulnerability scanning, penetration testing, password cracking, log review, integrity and configuration checkers, malicious code detection, and modem security. Often, several of these testing techniques are used in conjunction to gain more comprehensive assessment of the overall security posture. Testing should be designed to avoid any possible disruption to ongoing activities. Attacks, countermeasures, and test tools tend to change rapidly and often dramatically. Current information should always be sought. Testing will change along with changes in technology, threats, and needs.

KEYWORDS: Attacks, countermeasure, information system, IT, security, security testing, ST&E, testing

Acknowledgments

The author wishes to express thanks to the reviewers who improved the quality of this document. Special thanks to James A. Finegan.

Table of Contents

List of Figures

List of Tables

Executive Summary

Security testing and evaluation (ST&E) can lead to better security in information technology (IT) products and systems. The ST&E process can exert a strong, though indirect, positive effect on the initial specifications, the development process, the end product, and the operational environment. The purpose of this report is to assist the Federal Aviation Administration (FAA) in preparing for ST&E. ST&E occurs as part of (1) contractual acceptance, certification, and authorization of a new or enhanced system; and (2) recertification of existing, operational systems, sometimes called *legacy systems*, required periodically by FAA Order 1370.82. The FAA is planning to revise its Security Certification and Authorization (or Accreditation) (C&A) processes in fiscal year 2003. This report is intended to provide input to that revision and the supporting documents.

Best practices in system security testing are recommended in this report for adoption by the FAA. The objective of security testing is to validate the security functional and assurance requirements. A protection profile contains security functional specifications that define the objective security properties of the FAA System. A protection profile also contains security assurance specifications and other specifications of processes and procedures to be followed by the developer to provide assurance that the developed FAA System is sufficiently trustworthy. Assurance is the g rounds for confidence that the FAA System meets its security objectives. The most familiar security functional requirements are listed below; the full set of functional security requirements is discussed in Appendix D.

- Identification and Authentication
- Security Audit
- Security Management

The most familiar security assurance requirements are listed below; the full set is discussed in Appendix B.

- Configuration Management
- Development
  - Functional Specification
  - High-Level Design
- Guidance Documents
  - Security Administrator Guidance
  - User Guidance

Best practices in developmental system security testing are recommended in this report for adoption by the FAA. Several organizations in the FAA have responsibility for part of the ST&E process and can benefit from the comprehensive perspective of this report. Primary responsibility rests in the Product Team Information System Security (ISS) Management, the FAA Security Testing (Evaluation) Organization (ACB), and the ISS Policy and Guidance Organization (AIO/AIS).

The general scheme of ST&E is that the developer produces documentation describing the security properties of what was produced and how it was produced. The security properties are analyzed by the FAA using the functional specification, guidance documentation, and the high-level design of the system to understand the security behavior. The analysis is supported by independent testing of a randomly selected subset of the system security functions, evidence of developer testing based on the functional specification, selective confirmation of the developer test results, analysis of strength of functions, and evidence of a developer search for vulnerabilities.

The testing by the FAA may include a repetition of a subset of tests performed by the developer. The subset may be minimal if the results cause the FAA to gain confidence in the developer's performance. The amount of FAA testing is inversely proportional to the FAA's confidence. If testing and analysis does not inspire confidence, the FAA may repeat all the developer's testing and may also include tests beyond those conducted by the developer.

Testing includes the following types of security tests.

- Positive Tests—verify that the FAA System meets its specified security requirements.
- Negative Tests—verify that the FAA System does not do anything that is contrary to its security specifications. Testing should also insure that it does not have an adverse effect on any other FAA System.
- Vulnerability Tests—identify security vulnerabilities and modes of compromise in the FAA System.
- Penetration Tests—circumvent the security features of the FAA System.

Many assurance specifications relate to activities performed by the developer and documents (data items) produced by the developer. Some of these documents contain information that may be useful in the Security Testing and Evaluation process. Since ST&E occurs as part of contractual acceptance, the FAA test team should be part of the decision authorizing the formal, written approval required prior to final acceptance of the data item by the government.

Some testing of installed operational systems repeats testing of developmental systems, while other testing is unique to the operational in-service phase. The recommended testing methodology focuses first on those systems that are accessible externally (e.g., firewalls, web

servers) and then on other systems as resources permit. Attacks, countermeasures, and test tools tend to change rapidly and often dramatically. Current information should always be sought. The pedigree of tools must also be established.

The FAA should require a schedule and outline of deliverables from the developer in support of testing. Provision should be made for full regression testing of developer products. There is a tendency to omit regression testing from the schedule on the optimistic assumption that no flaws will be found and no rework will be required.

One important side effect of FAA analysis and testing is increased understanding on the architecture and design of the FAA System. The FAA must be vigilant to ensure that the scope of system testing is reflected in the developer's test plans. The security specifications to be tested should be drawn from the appropriate security specifications for the system with consideration of the enterprise and infrastructure.

The most important principle concerning roles and responsibilities is that there be separation of duties and a system of checks and balances. The specific organizations and their responsibilities could be changed without doing damage to this principle. The recommended roles and responsibilities for ST&E of developmental and legacy systems is summarized in Table ES-1. The abbreviations used in these tables are: AOS–Operational Support Service, IPT–Integrated Product Team, ISSM–Information System Security Manager, AIS–Information Security, ACB–Innovations & Solutions.

Table ES-1. ST&E Roles and Responsibilities

Function	Developmental System	Recertification
Create test plans	Developer	AOS
Approve test plans	IPT	ISSM
Conduct first testing	Developer	AOS
Verify first testing and conduct additional testing	AIS & ACB	AIS & ACB

Before actual testing, it is important to identify the resources required to execute the test procedures to ensure that they are available so that the testing can be conducted in a timely manner.

Security testing during proposal evaluation and the cost of testing are addressed. The cost of security testing of products and systems employing frequently used protocols, such as the Internet Protocol (IP) suite, is contrasted with the cost of security testing of products that implement protocols that are exclusively used by the aviation community. As shown in Table ES-2, rough order of magnitude cost estimates indicates that the cost of ST&E of non-

IP is prohibitive. The architecture should be arranged to make non-IP products untrusted and not security critical to avoid such costs.

Table ES-2. Rough Order of Magnitude Estimates for ST&E

Target of Evaluation (TOE)	Developer Preparation	Common Criteria Testing Laboratories (CCTL)	FAA Technical Center	Each FAA Field Site
COTS IP Firewall-Router	$750K borne by developer	$200K borne by developer	$20K borne by FAA	$5K borne by FAA
Non-IP Firewall-Router	$4M borne by FAA	$1M borne by FAA		$250K borne by FAA
NAS System	Included in development contract	$5M borne by FAA		$2.5M borne by FAA

Section 1

Introduction

1.1 Information Technology Security

Information Technology (IT) security is defined as the protection of information from unauthorized modification, loss of use, disclosure, or other undesirable threats arising from human or systems-generated activities, malicious or otherwise.

This report provides useful information and references that can be used to assist in planning and conducting security testing. The foundation starts with generally accepted ("Best") testing practices that are commonly used in security information technology (IT) community. This report should be viewed as high-level guidance that complements existing related documents.

Security Testing and Evaluation (ST&E) can lead to better IT security products in two ways. Firstly, evaluation is intended to identify errors or vulnerabilities in the Federal Aviation Administration (FAA) System that the developer may correct, thereby reducing the probability of security failures in future operation. Secondly, in preparing for the rigors of evaluation, the developer may take more care in FAA System design and development. Therefore, the evaluation process can exert a strong, though indirect, positive effect on the initial specifications, the development process, the end product, and the operational environment. ST&E is a special case of Test and Evaluation Verification, addressed in the *NAS System Engineering Manual* (FAA, 2002d).

The most common arrangement for system development is that the developer is an independent organization whose relationship to the FAA is governed by a contract. When this is not the case, the terms and obligations normally found in the contract should be contained in memoranda of agreement or other similar documents. The terms contract and contractor are used in this report without any loss of generality.

1.2 Background and Purpose of This Report

The purpose of this report is to assist the FAA in ST&E. Preparation for this report has included a survey of existing practice and guidance in the FAA and the Information Systems Security (ISS) community. It presents The MITRE Corporation's conclusions as to what constitutes "best practice" in ST&E and recommendations on implementation at the FAA. The principal source documents are cited so that the reader can trace back to original sources. The FAA is planning to revise its Security Certification and Authorization (or Accreditation) (C&A) processes in fiscal year 2003. This report is intended to provide input to that revision and the supporting documents. The most important principle concerning roles and responsibilities is that there be separation of duties and a system of checks and balances. The

specific organizations and their responsibilities could be changed without doing damage to this principle.

This report was produced as a follow-on activity to the development of the *National Airspace System (NAS) System Protection Profile Template* (SPPT)(March 2002a). As such, it assumes the existence of ISS specifications for the subject FAA System. This report addresses testing to assure that the implemented system conforms to the specifications. The *NAS SPPT* and its companion *Guidance* is one source that may be consulted concerning development of specifications. ISS can be tested only with respect to specifications; there are no absolutes. Activities encouraged in one environment may be prohibited in another. This report is independent of the specifications. Therefore, it is applicable to all FAA Systems.

One consequence of the *NAS SPPT* work is the recognition of the need for improvement in the incorporation of ISS thinking and procedures in the acquisition process. Separate activities are underway to modify the Acquisition Management System (AMS) and *FAA Acquisition System Toolset* (FAST). A protection profile contains security functional specifications that define the objective security properties of the FAA System. These functional specifications are properly placed as part of the system specification. A protection profile also contains security assurance specifications and other specifications of processes and procedures to be followed by the developer to provide assurance that the developed FAA System is sufficiently trustworthy. Assurance is the g rounds for confidence that the FAA System meets its security objectives. These specifications are properly placed as part of the Statement of Work (SOW), Contract Data Requirements List (CDRL), and Data Item Descriptions (DIDs). The developer's work in support of ST&E is part of the security assurance specifications in the SOW, CDRL, and DIDs.

In general, there are two separate activities requiring security testing – system contract acceptance and the production of the Security Certification and Authorization Package (SCAP). When the C&A process is not immediately preceded by system development, some of the activities assigned herein to the developer will be performed by the FAA. See Section 2 and Appendix B for further information. The contract acceptance testing should be a subset of the testing required for the SCAP.

Contract acceptance addresses only the functional and assurance security specifications contained in the contract with the developer. Testing required for the SCAP testing also includes physical and procedural security countermeasures implemented by the FAA. These FAA countermeasures may be assumed by the developer and may have been included as assumptions in a Protection Profile. Adequacy determination of the FAA security countermeasures as implemented is part of the testing required for the SCAP. Acceptance testing of the security properties of the developed FAA System is a prerequisite to security testing under the SCAP process.

At the time of writing, plans are underway for the FAA to adapt the National Information Assurance Certification and Accreditation Process (NIACAP) (NSTISC 2000). Current thinking is to incorporate the SCAP into the FAA's adoption of NIACAP. A general description of test and evaluation as part of the AMS is found in Appendix C.

1.3 Best Practice

In the government a very good source for "best practice" in security testing of operational systems is the National Institute of Standards and Technology (NIST) *Guideline on Network Security Testing*, Special Publication 800-42, which was available in draft at the time of this document's publication (Wack, 2002). This NIST Guideline describes a methodology for using network based tools for testing systems for vulnerabilities. The primary aim of the NIST Guideline is to help administrators and managers get started with a program for testing on a routine basis. The methodology recommends focusing first on those systems that are accessible externally (e.g., firewalls, web servers) and then moving on to other systems as resources permit. The NIST Guideline includes many pointers to various testing applications and contains detailed descriptions of several of the more popular test tools. The pedigree of tools must be established.

A second authoritative source is the *Common Evaluation Methodology* (CEM) (Common Criteria, 1999a) which is part of the *Common Criteria* (CC) (Common Criteria, 1999b). The Common Criteria is an international standard (ISO 15408) for certifying the security claims of IT products and systems. The CC contains an extensible set of criteria and procedures for independently evaluating the security properties implemented in IT products and systems. Security properties are divided into functional security properties, the security functions and protections implemented in the physical product or system; and assurance security properties, the grounds for confidence that the entity meets its security objectives. Assurance security properties include the development environment and process, manuals for secure operation and use, and other documentation about the developer and the product or system. Both functional and assurance properties are evaluated by analysis; only functional security properties can be tested The CC is implemented in the U.S. by the National Information Assurance Partnership (NIAP)[1], which has established the Common Criteria Evaluation and Validation Scheme (CCEVS). The CEM is a companion document to the CC, describing the minimum actions to be performed by an evaluator in order to conduct a CC evaluation using

---

[1] The National Information Assurance Partnership (NIAP) is a joint initiative of NIST and the National Security Agency (NSA) designed to meet the security testing needs of both IT producers and consumers. The partnership is intended to foster the availability of objective measures and test methods for evaluating the quality of IT security products. In addition, it is designed to foster the development of commercial testing laboratories that can provide the types of security testing and evaluation services which will meet the demands of both producers of IT products and consumers of those products.

the criteria and evaluation evidence defined in the CC. Additional information concerning CCEVS evaluations is found in Appendix A.

1.4 Testing Integrated Components

Most systems are built using other systems. Hardware platforms and operating systems, for example, are often purchased and used as the foundation on which applications are implemented. Let us assume that the hardware platforms and operating systems are Commercial-Off-The-Shelf (COTS) products. That is, they are offered for sale to the general public and not built specially for the FAA System.

The developer must determine the security properties of these components, whether COTS or government-furnished. The testing approach described in this report as applicable to the FAA System is recursively applicable to all the integrated components. In the best of all possible scenarios, the component will have been evaluated under CCEVS. If unevaluated components are used, the developer must perform some amount of testing on the unevaluated components to determine the security properties of the components and the way these security properties affect the integrated system. The assurance derived from the documentation accompanying the unevaluated components will affect the testing program required. When available, the actual code should be reviewed since documentation frequently can not be relied upon. Unavailability of code limits the assurance that can be placed in the component. Testing the security properties of the integrated components and the components developed by the developer is all part of the developer's testing program.

The FAA should make no distinction in verifying the developer's testing of integrated components or components wholly implemented by the developer. Components supplied by the FAA must be afforded no special treatment.

1.5 Security Policy Requirements

FAA Order 1370.82, *FAA Information Systems Security Program* establishes policy and assigns organizational and management responsibilities to ensure implementation of applicable Federal law and guidance.

The FAA Information System Security Architecture (ISSA) is a top-level design for integrating security into FAA IT, a set of alternatives for investment analysis, and a phased roadmap for responding to laws, directives, and policies imposed on Federal agencies. The ISSA helps provide a cost effective structure to assure that key security services are available and can be implemented in all of the FAA systems as needed. Requirements are strategically grouped into computer platform, communications, and management/administration categories. The ISSA focuses on the National Airspace System (NAS), but provide some guidance for Administrative and Mission Support (A&MS) systems.

The ISSA uses requirements defined by previous policy, threat, vulnerability and risk assessments to derive security service specifications. Vulnerability analyses indicate what and where security services are needed to preclude interference with safe and continuous operations. Threat assessments underscore the need for security services by revealing mechanisms capable of exploiting vulnerabilities. Risk assessment shows how extensively and when security services are needed by comparing the operational impact of vulnerability-threat combinations.

The FAA is responsible for ensuring that all of its information systems are protected from threats to integrity, availability, and confidentiality commensurate with the risk. Safety criticality, proprietary rights, privacy, and other rights and objectives also apply to different sets of information. In order to maintain the safety of the civil air transportation system and the public confidence, the FAA has ISS plans and goals to:

- Implement FAA Systems with security measures commensurate with criticality of resources.
- Develop an FAA information security management structure, approach, and architecture.
- Formalize information security engineering as an integral element of program development.
- Provide guidelines for information security-related investment decisions.
- Establish an evolutionary and continuing information security improvement program.
- Broaden awareness of the evolving information security vulnerabilities and countermeasures.

ISS policy (FAA Order 1370.82[2]) and the ISSA[3] are the drivers for ISS in the FAA. However, they provide little or no guidance for ST&E, hence the need for this report.

1.6 Scope of Concern

The scope of security engineering is not limited to the tangible assets of the FAA System, or the intangible data stored and processed, or even the entire FAA IT infrastructure, but for the ability of the FAA to perform its mission. The FAA System must provide the level of protection required for managing threats with the objectives that:

---

2 Section 13. a (15) requires that security test and evaluation be conducted for all ISS requirements and risk mitigation controls. Section 13. b (18) addresses penetration testing

3 Testing requirements occur frequently in Section 3.

- The FAA System cannot become a vehicle for attacking other enterprise systems.
- The FAA System cannot be used to decrease the availability of other enterprise systems.
- The security posture of the set of all the enterprise systems will not be decreased when the FAA System has become operational.

All of these objectives should be taken into account when writing the PP for the system. ST&E verifies that the implementation satisfies the specifications.

The FAA System may depend on other parts of the enterprise infrastructure for countermeasures against known threats. For example, firewalls at the NAS periphery, where it interfaces with networks outside the FAA security domain, may be expected to provide protection against a set of network-based attacks. This assumption should be documented in the Protection Profile. Such assumptions should be verified (e.g., by checking that another program has done ST&E on them). ST&E is part of the verification process.

System checkout tests addressed in Appendix D include tests that verify that the system is correctly integrated with specified interfaces and tests that verify that the newly installed equipment is correctly interfaced with the FAA IT infrastructure and that the infrastructure continues to function as before, after the FAA System is installed.

1.7 System Acceptance Activities

The expression of FAA System security specifications in documents, such as a Protection Profile (PP), System Specification Document (SSD), System Subsystem Specifications (SSS), Statement of Work (SOW), Contract Data Requirements List (CDRL), and Data Item Descriptions (DIDs), define the functional and assurance security specifications that the FAA System and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the FAA System.

When an existing FAA System, sometimes termed a legacy system, is presented for C&A, the roles and responsibilities need minor adjustment. Following CC terminology, the organization that initiates the C&A activity is termed the sponsor. The sponsor may be an Integrated Product Team (IPT), or similar organization, consisting of the organization that owns and operates the FAA System and the other stakeholders. The sponsor is responsible for developing the security specifications. Acceptable forms include PP, SSD, SSS, or equivalent. Assurance security specifications, and other specification that would be placed in the SOW for a contract, are placed in a companion document such as a separate section of the SSS or equivalent.

Validation of these specifications is performed by a separate group, perhaps an IPT, staffed by personnel from the sponsor and Information Security (AIS).

Security specifications generally include both specifications for the presence of desired behavior and specifications for the absence of undesired behavior. It is normally possible to demonstrate, by use or testing, the presence of the desired behavior. It is not generally possible to perform a conclusive demonstration of absence of undesired behavior. Testing and evaluation of documentation of all relevant processes, design, and implementation contribute significantly to reducing the risk that such undesired behavior is present.

The principal inputs to FAA System evaluation include:

- Deliverables specified in SSD, SOW, CDRLs, and DIDs
- Other contractual obligations such as the PP and contractor's proposal

Evaluation, analysis, and testing are tightly coupled. See Section 2 and Appendixes B and C. Analysis is directed to the deliverables specified in the SOW, CDRLs, and DIDs. These deliverables are referred to as data or as information. It is instructive to note that the Common Criteria (CC) (Common Criteria, 1999) tasks the evaluator to:

- Confirm that the information provided meets all requirements for content and presentation of evidence.
- Confirm that the information provided is complete, coherent, internally consistent, and consistent with other information provided.

The SOW specifies actions and deliverables by the developer of the FAA System that support security acceptance testing. The DIDs specify the content of these deliverables. The clauses in the *SPPT* that become SOW and DIDs are shown in Appendix H. Note: In this document the *NAS SPPT* can be understood to be an example of a structured expression of security conditions and specifications.

1.8 Document Organization

This document consists of six major sections and several appendices. Section 1 provides an introduction, defines the purpose and scope of the document, defines Security Testing and Evaluation (ST&E), addresses security requirements and their basis in policy. Section 2 addresses security testing practices for newly developed or modified systems as well as legacy systems undergoing recertification. Roles and responsibilities are also addressed. Section 3 addresses the special issues of security testing during proposal evaluation, testing tools, and the impact of architectural decisions on testing. Section 4 contains the summary and recommendations. References follow Section 4. A glossary follows the supporting appendices:

- Appendix A describes the Common Criteria Security Evaluation Scheme.
- Appendix B details Acceptance Testing Activities and Methodology.

- Appendix C describes *FAA Acquisition System Toolset* (FAST) and Security Testing.
- Appendix D describes the Security Test and Evaluation Process.
- Appendices E, F, and G contain examples of the Security Test Report Template, Security Test Plan Procedure Template, and Security Test Report Template, respectively.
- Appendix H presents typical FAA System Security Specifications.

Section 2

System Security Testing Practices

These security testing practices are commonly accepted practices that are currently employed in the computer security community. They do not take into account environmental or technological constraints, nor are they relevant to every situation. The information presented in this section is not intended to be all-inclusive and does not replace any FAA specific security testing guidance and/or policies. Some testing techniques are predominantly human-initiated and conducted. Other tests are highly automated and require less human involvement. Regardless of the type of testing, staff that setup and conduct security testing should have significant security and network system knowledge.

Recommendations concerning roles and responsibilities identify two roles in ST&E. The first role is to design and conduct testing and evaluation. The second role is to provide Independent Validation and Verification (IV&V) of the ST&E. In the context of C&A, this second role is part of certification. Role assignments to FAA organizations for developmental systems and recertification conclude this section.

2.1 Best Practices

Best practices are the commonly accepted practices that are generally employed today. See Section 1.3. The best security practices provide a common ground for determining the security of a system and build confidence in implementing and assessing security countermeasures. They show what should be done to enhance or measure an existing information system's security.

Best practices for testing of systems under development during the Solution Implementation Phase and in operation during the In-Service Management Phase are presented in the following two sections.

2.2 Developmental Systems

2.2.1 External Guidance and Resources

As introduced in Section 1.3 and elaborated in Appendix A, one of the best sources for best practice in security testing of systems while in development is the CCEVS based on the CEM to evaluate the security properties of IT products and systems. The analysis and testing addresses the assurance areas specified in the CC incorporated in the *SPPT* and used as the basis for FAA System security specifications.

While the CC and CEM have provided an excellent base to build upon, the FAA use of the SPPT is distinct from the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) which is a government-wide product evaluation program. CCEVS procedures and processes are independent of the FAA's purpose in utilizing the PP format for expressing security requirements and specifications.

The commercial testing laboratories accredited by NIST's National Voluntary Laboratory Accreditation Program (NVLAP)—called Common Criteria Testing Laboratories (CCTL)—are a valuable resource. When the FAA decides to contract out ST&E activities, some of these labs may be willing and able to help the FAA outside the CCEVS context to determine whether a FAA System is secure enough for its intended application and whether the residual security risks implicit in its use are acceptable.

NIAP also has initiated a new collaborative project to produce comprehensive Protection Profiles in key technology areas such as operating systems, firewalls, smart cards, biometrics devices, database systems, public key infrastructure components, network devices, virtual private networks, intrusion detection systems, and web browsers. The project objectives are:

- To ensure the U.S. Government has a consistent, seamless, comprehensive set of recommended protection profiles for each key technology area.
- To work with other stakeholders in the government and commercial sector in developing and vetting protection profiles for key technology areas.
- Facilitate national and international convergence of protection profiles for key technology areas.

These PPs will be available at http://niap.nist.gov/niap/services/security-specs.html and/or http://niap.nist.gov/cc-scheme/PPRegistry.html. This work is evolving at the time of writing.

2.2.2 Developmental System Security Testing

Best practice in developmental system security testing, employed in the Common Criteria Evaluation and Validation Scheme for Information Technology Security (NIAP, 1999), is recommended in this report for adoption by FAA. Details are presented in Appendix B. The security functional requirements include:

- **Identification and Authentication.** Identification and Authentication address functions to establish and verify a claimed identity. These functions are required to ensure that entities are associated with the proper Security Attributes (e.g., identity, groups, roles, confidentiality or integrity levels).
- **Security Audit.** Security auditing involves recognizing, recording, storing, and analyzing information related to security relevant activities (i.e., activities controlled

by the NAS System Security Policy). The resulting audit records can be examined to determine which security relevant activities have taken place and which entity is responsible for them.

- **Security Management.** Security Management is intended to specify the management of several aspects of the NAS System: security attributes, data, and functions. The different management roles and their interaction, such as separation of capability, are specified.
- **Cryptographic Support.** The NAS System may employ cryptographic functionality to help satisfy several high-level security objectives. These include (but are not limited to): identification and authentication, non-repudiation, trusted path, trusted channel, and data separation.
- **Network Security Protection.** Network Security Protection addresses the responsibility for maintaining the overall security posture of a NAS network.
- **Application Data Protection.** Application Data Protection specifies specifications for NAS System security functions and related policies for protecting NAS System application data.
- **Protection of Security Data and Mechanisms.** Protection of the NAS System Security Data and Mechanisms addresses the integrity and management of the data and mechanisms that implement the NAS System Security Policy.
- **Resource Utilization.** Resource Utilization supports the availability of required resources such as processing capability and/or storage capacity.
- **User Session Access Control.** NAS System Access specifies functional specifications for controlling the establishment of a user's session.
- **Trusted Path.** Trusted Path defines the specifications to establish and maintain trusted communication to or from users and the NAS System. A trusted path may be required for any security-relevant interaction. Trusted path exchanges may be initiated by a user during an interaction with the NAS System, or the NAS System may establish communication with the user via a trusted path.
- **Data Management.** Data Management specifies compliance with FAA Order 1375.1C, *Data Management* and FAA Order 1200.22C, *NAS Data and Interface Equipment Used by Outside Interests*
- **Internet Access.** Internet Access specifies compliance with FAA Order 1370.83, *Internet Access Points* and FAA Order 1370.84 *Internet Services.*

The security assurance requirements include:

- **Configuration Management.** Configuration Management (CM) is one method or means for establishing that the functional requirements and specifications are realized in the implementation. CM meets these objectives by requiring discipline and control in the processes of refinement and modification of the NAS Subsystem and the related information. CM systems are put in place to ensure the integrity of the portions of the NAS Subsystem that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorized.
- **Delivery and Operation.** Delivery and operation specifications address the measures, procedures, and standards concerned with secure delivery, installation, and operational use of the NAS System, ensuring that the security protection offered by the NAS System is not compromised during transfer, installation, start-up, and operation.
- **Development.** Development specifications address the stepwise refinement of the NAS System from the summary specification down to the actual implementation.
  - **Functional Security Specification.** The functional security specification is a high-level description of the user-visible interface and behavior of the security functions of the NAS System. The functional security specification has to show that all the NAS System security specifications are addressed.
  - **High-Level Security Design.** The high-level security design of the NAS System provides a description of the security properties in terms of major structural units (i.e., subsystems) and procedures, and addresses the adequacy of the security functions provided. The high-level security design specifications are intended to provide assurance that the NAS System provides an architecture appropriate to meet the security objectives.
- **Guidance Documents.** These specifications are directed at the understandability, coverage, and completeness of the operational documentation provided by the developer.
  - **Security Administrator Guidance.** Administrator guidance refers to written material that is intended to be used by those persons responsible for configuring, maintaining, and administering the NAS System in a correct and secure manner. Because the secure operation of the NAS System is dependent upon correct performance, persons responsible for performing these functions are necessarily trusted. Security administrator guidance is intended to help security administrators understand the security functions provided by the NAS System, including both those functions that require the security administrator to perform security-critical actions and those functions that provide security-critical information.

- **User Guidance.** User guidance refers to material that is intended to be used by non-administrative users of the NAS System, and by others (e.g., programmers) using NAS System external interfaces. User guidance describes the security functions provided by the NAS System and provides instructions and guidelines, including warnings, for its secure use. The user guidance provides a basis for assumptions about the use of the NAS System and a measure of confidence that non-malicious users, application providers, and others exercising the external interfaces of the NAS System will understand the secure operation of the NAS System and will use it as intended.

- **Developer and FAA Testing.** Testing demonstrates whether the NAS System satisfies the security functional specifications.
  - **Analysis of Coverage.** This specification addresses those aspects of testing that deal with completeness of test coverage. The objective is to establish that the NAS System has been tested against its security functional specification in a systematic manner. It addresses the extent to which the NAS System Security Function is tested, and whether or not the testing is sufficiently extensive to demonstrate whether the NAS System Security Function operates as specified.
  - **Analysis of Developer's Functional Tests.** Depth deals with the level of detail to which the developer tests the NAS System. The objective of testing is to counter the risk of missing an error in the development of the NAS System. Testing that exercises specific internal interfaces can provide assurance not only that the NAS System exhibits the desired external security behavior, but also that this behavior stems from correctly operating internal mechanisms. Testing at the level of the system components, in order to demonstrate the presence of any flaws, provides assurance that the NAS System components have been correctly implemented and integrated.
  - **Independent Testing.** Independent testing demonstrates whether the security functions perform as specified and helps counter the risk of an incorrect assessment of the test outcomes on the part of the developer that results in the incorrect implementation of the specifications, or overlooks code that is non-compliant with the specifications.

- **Vulnerability Assessment.** Vulnerability Assessment defines specifications directed at the identification of exploitable vulnerabilities introduced in the architecture and design, construction, operation, misuse, or incorrect configuration of the NAS System.
  - **Strength of Security Functions.** Strength of function analysis addresses security functions that are implemented by a probabilistic or permutational mechanism (e.g., a password or hash function). Even if such functions cannot be bypassed,

deactivated, or corrupted, it may still be possible to defeat them by direct attack because there is a vulnerability in the concept or implementation of its underlying security mechanisms.

– **Developer Vulnerability Analysis.** Developer vulnerability analysis is performed by the developer to ascertain the presence of vulnerabilities that could allow users to violate the NAS System Security Policy or reduce the security of any other part of the NAS, and to confirm or not confirm that they cannot be exploited in the intended environment.

The general scheme of ST&E is that the developer produces documentation describing the security properties of what was produced and how it was produced. The scope of acceptance testing includes the hardware and software implementing the FAA System and the documentation describing design, implementation, and security testing.

Security testing includes the following types of tests:

- Positive Tests—tests designed to verify that the FAA System meets its specified security requirements.
- Negative Tests—tests designed to verify that the FAA System does not do anything that is contrary to its security specifications. Testing should also insure that what it does will not have an adverse effect on any other FAA System.
- Vulnerability Tests—tests designed to identify security vulnerabilities and modes of compromise in the FAA System.
- Penetration Tests—tests designed to circumvent the security features of the FAA System.

2.2.3 Roles and Responsibilities

As part of a system of checks and balances to foster objectivity and uniformity, there are two roles in ST&E. The first role is to design and conduct testing and evaluation. The second role is to provide Independent Validation and Verification (IV&V) of the ST&E. In the context of C&A, this second role is part of certification.

The Integrated Product Team (IPT), or similar organization responsible for the developmental system, and the developer are responsible for the first role–establishing the security test plans and conducting developer testing. Typically there would be a contractual obligation for the developer to produce the security test plans and for the IPT to review and accept these plans. The developer would conduct the testing with some degree of IPT oversight.

Selection of test tools should be part of the test plan. Selection criteria include capabilities and cost/effectiveness. Public domain tools, including shareware and open

source, must also be scrutinized to ensure the absence of malicious content. Tools could be Trojan Horses.

Many assurance specifications relate to activities performed by the developer and documents (data items) produced by the developer. Some of these documents contain information that may be useful in ST&E.

The CC uses the term *evaluator* to describe a function similar to IV&V that embodies the second role. The CC contains criteria to be used by evaluators when forming judgments about the conformance of products and systems to their security requirements. The CC describes the set of general actions the evaluator is to carry out and the security functions on which to perform these actions. Note that the CC does not specify procedures to be followed in carrying out those actions.

The CC also observes that in order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative evaluation scheme that sets the standards, monitors the quality of the evaluations, and administers the regulations to which the evaluation facilities and evaluators must conform.

These principles are directly applicable to the FAA. In recognition of this, the report refers to the FAA evaluator. (Order 1370.82 assigns responsibility as the ISS Certification Agent for all FAA information systems to AIO, which has delegated it to AIS.) The testing part of that second role may be delegated to the FAA Security Testing (Evaluation) Organization (ACB). It is reasonable to think of ACB evaluating the depth and breadth of developer/IPT test plans, verifying the efficacy and trustworthiness of the test tools, observing developer testing, and performing testing on behalf of AIS. FAA evaluator test plans and results must be documented sufficiently to support flaw remediation and regression testing. ACB would prepare test plans and reports and AIS would review these documents. ACB and AIS would constitute the FAA security test team. This FAA security test team supports the Information Systems Security Certifier identified in FAA Order 1370.82.

The security properties are analyzed by the FAA evaluator using the functional specification, guidance documentation, and the high-level design of the system to understand the security behavior. The analysis is supported by the FAA evaluator conducting independent testing of a randomly selected subset of the system security functions, evidence of developer testing based on the functional specification, selective confirmation of the developer test results, analysis of strength of functions, and evidence of a developer search for obvious vulnerabilities. Further assurance is gained through a configuration list for the system and evidence of secure delivery procedures.

The test and evaluation performed by the FAA evaluator may include a repetition of a subset of tests performed by the developer. The subset may be minimal if the results cause the FAA evaluator to gain confidence in the developer's performance. The amount of FAA testing is inversely proportional to the FAA evaluator's confidence. If testing and analysis

does not inspire confidence, the FAA evaluator may repeat all the developer's testing and may also include tests beyond those conducted by the developer.

2.3 Operational System Testing

2.3.1 External Guidance and Resources

Existing, operational systems, sometimes called *legacy systems*, require periodic recertification. Recertification and reauthorization are required by FAA Order 1370.82:

- Every 3 years
- If there is a major system or environmental change that impacts the security posture of the system, including:
  - New or additional connectivity to other information systems
  - Major hardware/software changes
  - Whenever a major security breach has occurred

Some testing of installed operational systems repeats testing of developmental systems while other testing is unique to the operational in-service phase. As mentioned previously. NIST has developed a *Guideline on Network Security Testing*, Special Publication 800-42, which was available in draft at the time of this document's publication (Wack, 2002). This NIST Guideline describes a methodology for using network based tools for testing systems for vulnerabilities. The primary aim of the NIST Guideline is to help administrators and managers get started with a program for testing on a routine basis. The methodology recommends focusing first on those systems that are accessible externally (e.g., firewalls, web servers) and then moving on to other systems as resources permit. The NIST Guideline includes many pointers to various testing applications and contains more detailed descriptions of several of the more popular test tools. The reader is cautioned that attacks, countermeasures, and test tools tend to change rapidly and often dramatically. Current information should always be sought (e.g., from sources of known public domain weaknesses such as those published by activities such CERT and bugtraq).

2.3.2 FAA Testing Guidance Documents

Every effort has been made to ensure consistency with the applicable FAA testing guidance documents described below. However, all these documents are subject to revision. The reader should consult the most current version. This report is not an FAA publication. While it provides advice and guidance, it is not intended to supercede any FAA publication or policy.

The FAA ISS Handbook (FAA, 2002b) was written to provide a framework for satisfying the requirements set forth in Federal and FAA policy, such as FAA Order 1370.82. This

handbook was written with the goal to provide a consistent process to follow for system certification and authorization, and to offer a means for enhancing information systems security organization-wide by incorporating effective current practices and addressing weaknesses and gaps where necessary. The FAA ISS Handbook defines a 5-phase approach to meet the ISS security requirements. This approach is designed to accommodate the SCAP requirements. In addition, the handbook includes templates for required documents that must be produced for the SCAP.

The FAST includes the *Acquisition Management System Test & Evaluation Process Guidelines* (FAA, 2002c), which provide a sound foundation for planning and executing test and evaluation activities that are appropriate for each individual acquisition program. The AMS System Test & Evaluation Process Guidelines is applicable to a full-scale development, COTS procurement, or Operational Prototype. The AMS empowers Integrated Product Teams (IPTs) and Business Service Organizations (BSOs) to decide how FAA Systems will be acquired and how requirements will be verified (tested). AMS also contains information on best practices and lessons learned from previous and ongoing acquisition programs that are applicable to the ISS testing.

Appendix C provides extracts from the *Acquisition Management System Test & Evaluation Process Guidelines* that expresses fundamental FAA requirements for security acceptance testing. Citations for safety are included because of the extremely close relationship of safety and security. The In-Service Management phase illustrated in Figure C-1 provides an appropriate home for recertification ST&E.

Both the FAA ISS Handbook and AMS are recommended sources for planning ISS testing. Some of security testing guidelines from the FAA ISS Handbook and AMS are cited throughout this document.

2.3.3 Roles and Responsibilities

Typically, the ownership and maintenance of an operational system vests in Operational Support Service (AOS). Therefore, AOS is responsible for developing the security test plans and conducting recertification testing. The IPT may still be involved with the system, in which case they might share responsibility with AOS. The Information Systems Security Manager (ISSM) could perform the function of reviewing and accepting these plans. AOS would conduct the testing.

The FAA evaluator role and FAA test team would be the same for Operational System Testing as for Developmental System Testing.

2.4 Summary of Roles

The recommended roles and responsibilities for ST&E of developmental and legacy systems is summarized in Table 2-1. As mentioned, the most important principle concerning

roles and responsibilities is that there be separation of duties and a system of checks and balances. The specific organizations and their responsibilities could be changed without doing damage to this principle.

Table 2-1. ST&E Roles and Responsibilities

Function	Developmental System	Recertification
Create test plans	Developer	AOS
Approve test plans	IPT	ISSM
Conduct first testing	Developer	AOS
Verify first testing and conduct additional testing	AIS & ACB	AIS & ACB

Section 3

Special Issues

Four topics, which were raised during the initial analysis and document review, are addressed in this section:

- Security Testing During Proposal Evaluation
- Testing Tools
- Architecture Testing
- Penetration Testing

3.1 Security Testing During Proposal Evaluation

A certain amount of test and evaluation may occur as part of proposal evaluation. Benchmarking and functional demonstrations are traditionally employed. Benchmarking has included stress testing (e.g., response time, throughput), that is similar to some security testing. Selecting the breadth and depth of such benchmarking is a business decision. Both the FAA, as purchaser, and offeror incur costs. Either party may decide that the costs are prohibitive. It may be possible to structure proposal evaluation to limit the number of proposals which receive intensive ST&E. For example, security functional demonstrations could be required of all offerors, while assurance and penetration testing could be applied to only the apparent selectee.

There is significant difference among ST&E of existing products, systems to be developed, and services. Systems to be developed and services share a degree of uncertainty of looking into the future. One approach is to consider whether failure to deliver the proposed security functions, assurances, and services amounts to breach of contract for which there are various legal remedies. The FAA can structure the pre-award functional demonstrations so that they provide meaningful and consistent results for evaluation purposes.

3.2 Testing Tools

Testing tools are available from commercial and non-commercial sources. The tradition of sharing is alive and well in the security auditing, testing, and scanning community. The FAA evaluator must exercise due diligence in selecting tools. It is known for malicious code to be hidden in such tools, thereby creating a Trojan Horse. One way to check the pedigree of tools is to refer to web pages used to exchange information among this community. For example, http://www.insecure.org/ maintains the results of a survey of the top 50 security tools and an archive of security information exchange lists and forums.

3.3 Architecture Relationship to Testing Costs

The relationship of architecture to testing cost is somewhat contentious, because it may involve the network layer of the Aeronautical Telecommunications Network (ATN) protocol suite, an International Civil Aviation Organization (ICAO) standard (ICAO, 2002). This report frames the issue as the cost impact of ST&E of products implementing a network layer communications protocol other than the widely used standard Internet Protocol (IP) suite of protocols, referred to as IP for convenience in this report. Our experience with ATN is used as our primary source for the information in this matter.

The architecture and design have severe impact on threats, countermeasures, and testing. This section focuses on the security testing implications, especially the cost of testing, of substantial reliance on systems and services that have no security pedigree. Good design includes testability as a criteria. This section focuses on minimizing the cost of ST&E by judicious architecture and design in minimizing the security impact of employing systems and services about which there is little or no knowledge concerning the security properties. Security architecture and design should employ techniques, such as encapsulation and isolation, and mechanisms, such as demilitarized zones and firewalls, to mitigate vulnerabilities and risks.

In other words, the system architecture, and especially the security architecture, can have a profound impact on cost. It is prudent to consider security costs in selecting an architecture. The use of Commercial-off-the-Shelf/Non-Developmental Item (COTS/NDI) significantly reduces all costs–research and development as well as ST&E.

External communications networks are presented as one example. Service-provider air-to-ground and ground-to-ground networks must be treated as untrusted unless adequate security properties have been established. The Designated Approving Authority (DAA) is responsible for approving connection to such external networks.

The cost impact of the choice of telecommunications protocol is another example. The Internet Engineering Task Force (IETF) has been actively developing security standards for IP. Systems and services implementing the most recent IETF security protocols are more trustworthy than those that do not. There is a very active market for IP implementations. Usage and competitive market forces help identify security weaknesses, supplementing formal ST&E. In contrast, systems using technology that is not in the mainstream of market products lack both modern security standards and an active competitive marketplace. Recognizing the controversial nature of any discussion of ATN, this report focuses on cost avoidance associated with the security characteristics of obscure protocols, drawn from our experience with ATN network layer protocol. This section estimates the cost of testing a developmental system. The costs of testing COTS/NDI products, non-COTS developmental products, non-IP products, and complete systems are presented. The analysis below shows that the cost of ST&E for non-IP is prohibitive. The architecture should avoid trusting non-IP products.

The "security through obscurity" argument may be valid when applied to hackers and other attackers with limited resources or motivation (e.g., so-called script kiddies). In contrast, state-sponsored terrorists and information warriors would not find ATN to be obscure. All the ATN standards and the few existing implementations are available to all ICAO members, including nation-states openly hostile to the United States.

The depth and breadth of security testing of the implementation of non-IP protocols depends on a vulnerability analysis of the chosen architecture. As discussed above, some architectures could reduce the security relevance of the non-IP implementation. In this section we discuss non-IP as if it were fully trusted in order to make a worst case cost estimate. We make conservative estimates of the relative cost of non-IP testing as compared to the more familiar IP protocols. It has been suggested that "equivalent testing should have equivalent costs." This might be true if the test resources were equal for testing both protocol suites. This is not the case. There is extensive experience with tools available for IP; there is nothing comparable for non-IP. There would be a cost associated with non-IP skill development and tool building that would have to be borne by the FAA.

3.3.1 Testing Cost Estimates

Some data are available concerning the cost of IT security evaluations conducted by commercial testing laboratories accredited by NIST's National Voluntary Laboratory Accreditation Program (NVLAP) called Common Criteria Testing Laboratories (CCTL). See Appendix A for a detailed description of NVLAP.

The CCTL testing paradigm is for evaluation to be conducted by a licensed laboratory on a fee-for-service basis. The total cost to the product developer also includes the preparation for evaluation above and beyond normal product development and marketing. It is instructive to use CCTL costs as a basis and then apply a multiplicative factor for additional costs due to the uniqueness of non-IP. The following conservative and illustrative estimates are used to produce a rough order of magnitude estimate for non-IP security testing. Public domain costing information has been used whenever possible.

Computer Science Corporation (CSC) is one of the CCTL. They had performed the evaluation of the CISCO 520 firewall product. CSC stated that the cost of evaluating such a firewall product is quite sensitive to the assurance level of the evaluation. They indicated that to perform an Evaluation Assurance Level (EAL) 3 of a firewall the cost would be between 170 to 200 thousand dollars ($170K-200K). The cost of EAL 2 would be about 25 thousand dollars ($25K) less while EAL 4 would be about 50 thousand dollars ($50K) more. While the *NAS SPPT* does not use the EAL scale, EAL 3 is a reasonable costing point.

The cost of developer preparation and CCTL testing for a COTS/NDI product is initially borne by the developer and assumed to be amortized over the customer base by incorporation in the product price. Historically, availability of the evaluated product has lagged the non-evaluated product due to the time consumed in the evaluation process, and has been priced at

an often considerable premium. For commercial products that were not explicitly designed for CCTL testing, the cost of preparation is typically an order of magnitude more than the cost of evaluation. This is especially true at the EAL4 level, where significant design documentation does not exist in a commercial product, but must be created to a significant level of detail. The cost of preparation and testing for a non-COTS developmental item would be borne directly by the FAA.

Testing in a CCTL laboratory would be followed by testing in the simulated production environment of the FAA William J. Hughes Technical Center (WJHTC). A relatively simple security product, such as a firewall, will require configuration and limited testing because it does not directly interact with FAA systems. In contrast a more complicated boundary protection device, such as an applications proxy that does interact with FAA system, will require more extensive ST&E. We estimate the cost of WJHTC testing of the former at ten percent (10%) of the CCTL cost. The latter is estimated at equal cost based on repeating the CCTL testing in an environment that duplicates, as far as possible, the real life situations, connections, configurations, and use cases of deploying the product in the FAA.

If everything went well and no discrepancies were discovered, then the WJHTC testing might cost a small fraction of the CCTL testing. If WJHTC testing did not confirm CCTL testing, the cost would vary according to how much testing WJHTC decided to perform. There would certainly be increased costs for remediation and retesting that are excluded from this estimate.

Successful testing at WJHTC leads to type approval. The next step is testing at the FAA field site. All field sites are not equivalent; there is local customization that may impact security properties. Successful site testing should involve repetition of WJHTC testing in the actual environment. We estimate twenty five percent (25%) of WJHTC testing cost at each site. If site testing uncovers anomalies, the problem should be referred to WJHTC for resolution. The cost of field site testing is directly related to the variance among the field sites. Reducing variance would reduce ST&E costs.

Cisco Corporation stated that the cost to prepare the test documentation for CCTL for an EAL 4 evaluation of one of their products, would be between 500 and 750 thousand dollars ($500K - $750K). A firewall is much simpler than many other systems, since its security features are reasonably easy to define. Hence, the cost is lower than most other products. The developer's costs include revising the documentation into the format that the testing labs require and the developer testing. A breakdown of these two functions, documentation and testing, is around a 60 to 40 ratio. That is, sixty percent is for documentation and the forty percent for testing. If the product were to have an EAL 3 evaluation the cost would be about 100 thousand dollars ($100K) less.

3.3.2 Non-IP Testing Cost Escalation

As pointed out above, there would be a cost associated with non-IP skill development and tool building that would have to be borne by the FAA. A qualified tester must know the protocol in depth in order to test it and must have adequate test software. Qualified individuals are few. The FAA would bear the cost of training and tool development. We estimate these costs as a multiplier on the cost of equivalent TCP/IP testing. These estimates have a wide margin of error. The need for security testing of the non-IP implementation depends on the chosen architecture. An architecture that diminishes the security relevance of the non-IP implementation decreases the difficulty of testing required.

It is prudent to assume that the code for non-IP testing will have to be developed and tested before deployment in an FAA network. A factor of five is used for this estimate. The reason for such an increase is that there are very few programmers capable of developing code for non-IP protocols, there are few companies that currently use non-IP products and no testing labs now available to test such products. There are many options that non-IP can use that will require extensive testing to insure that they do not effect the NAS. The testing organization will have to develop an independent non-IP implementation. Using the same implementation in the test driver and target of evaluation (TOE) is not acceptable testing practice. Since there is essentially no market for non-IP products, we assume that all ST&E will be performed by the WJHTC, perhaps with assistance from a CCTL.

3.3.3 Additional Costs Due to Lack of non-IP Experience

IP implementations have been tested for at least twenty years by thousands of computer professionals in many different environments and there are still vulnerabilities being discovered almost monthly. Real-world product use is an excellent testing environment. The same experience should be anticipated for non-IP implementations, if there were an adequate user population. Since non-IP will not be widely deployed, an extensive testing program should be employed to duplicate insofar as possible the accumulated experience with IP.

All IP protocols are required to test two independent implementations of the protocol before the protocol can be accepted for full standardization. Interoperability of these two independent implementations is required. It is prudent to assume that non-IP protocols do not have even this level of demonstration.

These test estimates remain extremely high regardless of how the non-IP capability is architected. The level of testing and therefore the total cost should be as high as the estimates or actually increase, to insure an appropriate level of confidence that non-IP can be considered operational in the NAS environment.

3.3.4 Another Cost Data Point

Since most CCTL testing has been directed to products, these is little data to estimate the cost of ST&E for a system custom built for the FAA. The cost of preparing for a security evaluation is not often made public. Fortunately, one other data point is available. Jeremy Epstein (Epstein, 2001) managed the security evaluation of a network operating system product, which we will assume is closest to a system custom built for the FAA.

He estimates that over ten million dollars ($10M) was spent. This excludes the manufacturer's costs in preparation and remediation. These costs were under the evaluation scheme that preceded CCEVS at a level that is roughly comparable to what is now EAL3. That cost estimate also includes the cost of developing a comprehensive security test suite, which didn't exist for the product. Mr. Epstein reports that at the time (mid 1990s) no product evaluation had ever cost less than five million dollars ($5M) and 3 years, with ten million dollars ($10M) and 5 years being typical.

The rough order of magnitude estimates for ST&E are shown in Table 3-1.

Table 3-1. Rough Order of Magnitude Estimates for ST&E

Target of Evaluation (TOE)	Developer Preparation	Common Criteria Testing Laboratories (CCTL)	FAA Technical Center	Each FAA Field Site
COTS IP Firewall-Router	$750K borne by developer	$200K borne by developer	$20K borne by FAA	$5K borne by FAA
Non-IP Firewall-Router	$4M borne by FAA	$1M borne by FAA		$250K borne by FAA
NAS System	Included in development contract	$5M borne by FAA		$2.5M borne by FAA

3.4 Penetration Testing

Penetration testing has been described as the gold standard and acid test for information system security. This section summarizes issues and recommends that the FAA establish a policy for penetration testing. Additional detail is in Appendix Section D.9.3.

Penetration testing (pen test or PT) is testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The purpose of penetration testing is to identify vulnerabilities, not previously identified, by which an adversary could gain unauthorized access. It is assumed that once identified, the vulnerabilities can be repaired, redesigned, or otherwise protected.

Penetration testing can be an invaluable technique. This may be the only way to determine operational and configuration deficiencies. However, it is a very labor intensive activity and requires great expertise to minimize the risk to targeted systems.

PT is part of a continuum of security measures. In the order of decreased automation and increased cost and analysis, the measures are:

- Vulnerability scanning
- Vulnerability assessment
- Penetration testing

There are three degrees of freedom available for penetration testing (1) unsupervised, such as case where the evaluator is alone at a terminal; (2) partially supervised, such as the case where the evaluator is accompanied by a qualified system administrator; and (3) supervised, such as the case where the evaluator is under the direct control of a qualified system administrator.

Penetration testing can be overt or covert. These two types of penetration testing are commonly referred to as Blue Teaming and Red Teaming. Blue Teaming involves performing a penetration test with the knowledge and consent of the organization's IT staff. Red Teaming involves performing a penetration test without the knowledge of the organization's IT staff but with full knowledge and permission of the responsible management.

The use of PT in an operational, or production, command and control system, like the NAS, requires additional care and consideration. Utilization of penetration testing should be avoided if at all possible and only after less intrusive means have been exhausted. PT of the live production system may be the only way to discover configuration problems that involve multiple systems or that include the human-computer interface.

MITRE recommends that the FAA establish a policy for penetration testing in FAA Systems that balances the risks and benefits and provides uniform procedures, rules of engagement, and identified level of management authorization required.

Section 4

Summary and Recommendations

The number of components that must be trusted should be considered in selecting an architecture. Cost should always be one of the driving concerns in selecting an architecture. Security testing can be a major cost driver.

Best practice in security testing is recommended in this report for adoption by the FAA. Specific recommended sources are the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) based on the Common Evaluation Methodology (CEM) for testing developmental systems and the NIST *Guideline on Network Security Testing* for operational security testing. Specific recommendations include:

- Focus first on those systems that are accessible externally (e.g., firewalls, web servers) and then moving on to other systems as resources permit.
- Address the assurance areas specified in the Common Criteria – incorporated in the *NAS SPPT*
- The cost of ST&E of non-COTS is prohibitive. The architecture should be arranged to make non-COTS products untrusted and not security critical to avoid such costs.
- Utilization of penetration testing should be avoided if at all possible and only used after less intrusive means have been exhausted.
- The FAA should establish a policy for penetration testing in FAA Systems that balances the risks and benefits, provides uniform procedures, and identifies the level of management authorization required.

The security functions of developmental systems are analyzed using a functional specification, guidance documentation, and the high-level design of the system to understand the security behavior. Operational system security testing should be integrated into an organization's security program. The primary reason for testing an operational system is to identify potential vulnerabilities and subsequently repair them. The following types of testing are described in the Appendixes: network mapping, vulnerability scanning, penetration testing, password cracking, log review, integrity and configuration checkers, malicious code detection, and modem security.

The general scheme of ST&E is that the developer produces documentation describing the security properties of what was produced and how it was produced. The security properties are analyzed by the FAA using the functional specification, guidance documentation, and the high-level design of the system to understand the security behavior. The analysis is supported by independent testing of a randomly selected subset of the system

security functions, evidence of developer testing based on the functional specification, selective confirmation of the developer test results, analysis of strength of functions, and evidence of a developer search for obvious vulnerabilities.

The recommended roles and responsibilities for ST&E of developmental and legacy systems is summarized in Table 4-1. The most important principle concerning roles and responsibilities is that there be separation of duties and a system of checks and balances. The specific organizations and their responsibilities could be changed without doing damage to this principle.

Table 4-1. ST&E Roles and Responsibilities

Function	Developmental System	Recertification
Create test plans	Developer	AOS
Approve test plans	IPT	ISSM
Conduct first testing	Developer	AOS
Verify first testing and conduct additional testing	AIS & ACB	AIS & ACB

List of References[4]

Abrams, M. D., and P. H. Cratch, September 2001, *Information Systems Security (ISS) Testing Guidance for the Free Flight Program*, MITRE Technical Report, MTR 01W0000076, The MITRE Corporation, McLean, VA.

Common Criteria Project, *Common Criteria for Information Technology Security Evaluation*, version 2.1., 1999. Or, International Standard ISO/IEC 15408 (1999-12); Parts 1-3, Information Technology Security Techniques – Common Criteria for IT Security Evaluation (CCITSE). Available from: http://csrc.nist.gov/cc/, http://www.radium.ncsc.mil/tpep/library/ccitse/ccitse.html, or http://www.commoncriteria.org/cc/cc.html.

Common Criteria Project, August 1999, *Common Evaluation Methodology* (CEM), version 1.0, Available from http://www.commoncriteria.org/cc/cc.html.

Epstein, J, November 26, 2001, private communication.

Federal Aviation Administration, March 2002a, *National Airspace System (NAS) System Protection Profile Template*, draft version 1.0 (or most recent version). http://www.faa.gov/aio/ChiefSci/index.htm or http://www2.faa.gov/aio/common/documents/NAS_PP_Tmp_v1.pdf.

Federal Aviation Administration, February 2002b, *FAA Information Systems Security Program Handbook*, version 3 (or most recent version).

Federal Aviation Administration, April 2002c, "Acquisition Management System Test & Evaluation Process Guidelines", *FAA Acquisition System Toolset* (FAST), http://fast.faa.gov/test_evaluation/test_eval_toc.html.

Federal Aviation Administration, November 2002d, *National Airspace System System Engineering Manual*, version 1, http://www.faa.gov/asd/SystemEngineering/index.htm.

International Civil Aviation Organization, April 2002, *Comprehensive Aeronautical Telecommunication Network (ATN) Manual*, Edition 2, Document 9739 (draft).

National Information Assurance Partnership (NIAP), May 1999, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Organization, Management and Concept of Operations*, Scheme Publication #1 Version 2.0, Gaithersburg, MD. http://niap.nist.gov/cc-scheme/.

---

4 Internet addresses were verified at the time of publication, but may have changed.

National Security Telecommunications and Information Systems Security Committee (NSTISC), April 2000, *National Information Assurance Certification and Accreditation Process* (NIACAP), NSTISSI No. 1000, available at http://www.nstissc.gov/html/library.html.

Swanson, M., August 2001, *Security Self-Assessment Guide for Information Technology Systems*, National Institute of Standards and Technology, Special Publication 800-26. Available at http://csrc.nist.gov/publications/nistpubs/index.html.

Wack, J, and M. Tracey, February 2002, draft *Guideline on Network Security Testing*, National Institute of Standards and Technology, Special Publication 800-42. Available at (http://csrc.nist.gov/publications/nistpubs/index.html).

Appendix A

Common Criteria Evaluation and Validation Scheme

The following description of the Common Criteria Evaluation and Validation Scheme (CCEVS) is extracted from information available at http://niap.nist.gov/cc-scheme/.

A.1 Objectives

The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), through the joint National Information Assurance Partnership (NIAP), have the following objectives in developing, operating, and maintaining an evaluation and validation scheme:

- To meet the needs of government and industry for cost-effective evaluation of Information Technology (IT) products
- To encourage the formation of commercial security testing laboratories and the development of a private sector security testing industry
- To ensure that security evaluations of IT products are performed to consistent standards
- To improve the availability of evaluated IT products

The scheme is intended to serve many communities of interest with very diverse roles and responsibilities. This community includes IT product developers, product vendors, value-added resellers, systems integrators, IT security researchers, acquisition/procurement authorities, consumers of IT products, auditors, and accreditors (individuals deciding the fitness for operation of those products within their respective organizations).

A.2 IT Security Evaluation and Validation

Consumers of IT products, such as the Federal Aviation Administration (FAA), need to have confidence in the security features of those products. Consumers want to be able to compare various products to understand their capabilities and limitations. Confidence in a particular IT product can be based on the trusted reputation of the developer, past experience in dealing with the developer, or the demonstrated competence of the developer in building products through recognized assessments. The consumer could also test the product directly and obtain the necessary results. The first approach lacks measurable results and the second approach requires substantial, costly effort. When products are available commercial-off-the-shelf, the CCEVS offers an impartial assessment by an independent entity. This impartial assessment, or *security evaluation*, includes an analysis of the IT product and the testing of the product for conformance to a set of security requirements. IT security

evaluations are composed of analysis and testing, distinguishing these activities from the more traditional forms of conformance testing in other areas. The FAA must perform is own security evaluation and testing for unique one-of-a-kind systems developed for the FAA. CCEVS procedures can be adapted by the FAA to take advantage of best practice and standards.

It is important that security evaluations of IT products be carried out in accordance with recognized standards and procedures. The use of standard IT security evaluation criteria and IT security evaluation methodology[5] contributes to the repeatability and objectivity of the results but is not by itself sufficient. Many of the evaluation criteria require the application of expert judgment and background knowledge for which consistency is more difficult to achieve.

A.3 Common Criteria Testing Laboratories

IT security evaluations are conducted by commercial testing laboratories accredited by NIST's National Voluntary Laboratory Accreditation Program (NVLAP) and *approved* by the NIAP Validation Body. These approved testing laboratories are called Common Criteria Testing Laboratories (CCTL). The FAA may choose to employ a CCTL as part of its security testing team. In this context, the CCTL brings experience and expertise. FAA evaluation and testing does not necessarily follow the CCEVS. A list of current CCTLs may be found at http://niap.nist.gov/cc-scheme/TestingLabs.html.

CCTLs in the United States focus heavily on security testing. This appears to be driven by developers who contract with them. The developers are looking for test reports they can subsequently provide to current or potential customers. The CCTL's focus on other CC evaluation-related activities has been minimal to date.

---

5 The *Common Criteria for IT Security Evaluation* [COM98] and the *Common Methodology for IT Security Evaluation* [CEM99] are used as the standard evaluation criteria and evaluation methodology, respectively, for all security evaluations of IT products within the scheme. The Common Criteria is an international standard (ISO/IEC 15408).

Appendix B

Acceptance Testing Activities and Methodology

B.1 Introduction

This appendix provides more detail concerning the recommended activities and methodology for Security Test and Evaluation (ST&E). These recommendations have been extracted from Common Evaluation Methodology (CEM) (August 1999) associated with the Common Criteria (CC) and adapted for use by the Federal Aviation Administration (FAA). In general, the ST&E methodology described is applicable to any set of assurance specifications. Higher levels of assurance imply increased and more rigorous analysis, documentation, and testing, with commensurate cost and time increases. The analysis and testing described herein provides a low to moderate level of independently assured security. This level was chosen for consistency with the level of security assurance specifications in the *NAS SPPT*. Achieving even this level of assurance for legacy systems may be quite challenging. Higher levels of assurance can be specified by tailoring the *SPPT* to use higher levels from the CC. Cost-benefit analysis should support such tailoring and be recorded in the Protection Profile (PP) Rationale.

The security functions are analyzed using a functional specification, guidance documentation, and the high-level design of the system to understand the security behavior. The analysis is supported by independent testing of a subset of the system security functions, evidence of developer testing based on the functional specification, selective confirmation of the developer test results, analysis of strength of functions, and evidence of a developer search for obvious vulnerabilities. Further assurance is gained through a configuration list for the system and evidence of secure delivery procedures.

ST&E addresses the assurance areas specified in the CC – incorporated in the *NAS System Protection Profile Template (SPPT)* (FAA, 2002a) – listed below, followed by in-depth discussion.

- Configuration Management
- Delivery And Operation
- Installation, Generation And Start-Up
- Development
  - Functional Specification
  - High-Level Design
- Guidance Documents

  - Security Administrator Guidance
  - User Guidance
- Developer and FAA Testing
  - Analysis Of Coverage
  - Analysis Of Developer's Functional Tests
  - Independent Testing
- Vulnerability Assessment
  - Strength of Security Functions
  - Developer Vulnerability Analysis

B.2 Configuration Management[6]

The purpose of the configuration management activity is to assist the consumer in identifying the specific version of the system, and to ensure that configuration items are uniquely identified. This activity contains an implicit action to determine that the CM system is being used.

The FAA evaluator checks that the version of the system provided for testing is uniquely referenced. The FAA evaluator should use the developer's CM system to validate the uniqueness of the reference by checking the configuration list to ensure that the configuration items are uniquely identified. Evidence that the version provided is uniquely referenced may be incomplete if only one version is examined during the evaluation, and the FAA evaluator should look for a referencing system that is capable of supporting unique references (e.g., use of numbers, letters or dates). The FAA evaluator should seek to examine more than one version of the system (e.g., during rework following discovery of a vulnerability), to check that the two versions are referenced differently.

The FAA evaluator checks that the system provided for testing is labeled with its reference. The FAA evaluator should ensure that the system contains a unique reference such that it is possible to distinguish different versions of the system. This could be achieved through labeled packaging or media, or by a label displayed by the operational system. This is to ensure that it would be possible for consumers to identify the system (e.g., at the point of purchase or use). The system may provide a method by which it can be easily identified.

---

6 Some of specifications for which ST&E procedures are presented may be placed in acquisition documents somewhere other than the security section. This is because such specification has both security and non-security import. The placement in the solicitation does not effect the ST&E.

For example, a software system may display its name and version number during the start up routine, or in response to a command line entry. A hardware or firmware system may be identified by a part number physically stamped on the system.

The FAA evaluator checks that the system references used are consistent. If the system is labeled more than once then the labels have to be consistent. For example, it should be possible to relate any labeled guidance documentation supplied as part of the system to the operational system. This ensures that consumers can be confident that they have received the correct version of the system, that they have installed this version, and that they have the correct version of the guidance to operate the system. The FAA evaluator can use the configuration list that is part of the provided CM documentation to verify the consistent use of identifiers.

The FAA evaluator checks that the CM documentation provided includes a configuration list identifying the items being maintained under configuration control and determines that it describes how configuration items are uniquely identified. The FAA evaluator examines the configuration list to determine that it identifies the configuration items that comprise the system. The FAA evaluator assesses the adequacy of the list on the basis of the approach taken by the developer to CM. For example, when a change is made to the system or any item of documentation, the FAA evaluator may observe or enquire at what level of granularity the item is re-issued. This granularity should correspond to the configuration items that appear in the configuration list. The FAA evaluator checks that the configuration list uniquely identifies each configuration item. The configuration list contains a list of the configuration items that comprise the system, together with sufficient information to uniquely identify which version of each item has been used (typically a version number). Use of this list will enable the FAA evaluator to check that the correct configuration items, and the correct version of each item, have been used.

B.3 Delivery and Operation

The purpose of the delivery and operation activity is to judge the adequacy of the documentation of the procedures used to ensure that the system is installed, generated, and started in the same way the developer intended it to be and that it is delivered without modification. This includes both the procedures taken while the system is in transit, as well as the initialization, generation, and start-up procedures.

The FAA evaluator examines the delivery documentation to determine that it describes all procedures that are necessary to maintain security when distributing versions of the system or parts of it to the field site. Interpretation of the term “necessary” will need to consider the nature of the system. The level of protection provided should be commensurate with the assumptions, threats, organizational security policies, and security objectives. The FAA evaluator determines that a balanced approach has been taken, such that delivery does not present an obvious weak point in an otherwise secure development process. The delivery

procedures describe how to determine the identification of the system and to maintain integrity during transfer of the system or its component parts. The procedures describe which parts of the system need to be covered. It should contain procedures for physical or electronic (e.g., for File Transfer Protocol [FTP]) distribution where applicable. The delivery procedures refer to the entire system, including applicable software, hardware, firmware and documentation. Integrity will always be of concern for system delivery. Where confidentiality and availability of delivery are of concern, they also should be considered. The delivery procedures should be applicable across all phases of delivery from the production environment to the installation environment (e.g., packaging, storage and distribution).

The FAA evaluator examines the delivery procedures to determine that the chosen procedure and the part of the system it covers is suitable to meet the security objectives. The suitability of the choice of the delivery procedures is influenced by the specific system (e.g., whether it is software or hardware) and by the security objectives. Standard commercial practice for packaging and delivery may be acceptable. This includes shrink wrapped packaging, a security tape or a sealed envelope. For the distribution the public mail or a private distribution service may be acceptable.

The FAA evaluator examines aspects of the delivery process to determine that the delivery procedures are used. The approach taken by the FAA evaluator to check the application of delivery procedures will depend on the nature of the system, and the delivery process itself. In addition to examination of the procedures themselves, the FAA evaluator should seek some assurance that they are applied in practice. Some possible approaches are:

- A visit to the distribution site(s) where practical application of the procedures may be observed
- Examination of the system at some stage during delivery, or at the user's site (e.g., checking for tamper proof seals)
- Observing that the process is applied in practice when the FAA obtains the system through regular channels
- Questioning end users as to how the system was delivered

Where the FAA has not yet taken delivery of a newly developed system, appropriate procedures and facilities should be in place prior to delivery and all personnel involved made aware of their responsibilities. The FAA evaluator may request a "dry run" of a delivery if this is practical. If the developer has produced other similar products, then an examination of procedures in their use may be useful in providing assurance.

B.4 Installation, Generation, and Start-Up

The objective of this activity is to determine whether the procedures and steps for the secure installation, generation, and start-up of the system have been documented and result in a secure configuration. The installation, generation, and start-up procedures refer to all installation, generation, and start-up procedures, regardless of whether they are performed at the user's site or at the development site that are necessary to progress the system to the secure configuration as documented.

The FAA evaluator checks that the procedures necessary for the secure installation, generation and start-up of the system have been provided. The FAA evaluator examines the provided installation, generation, and start-up procedures to determine that they describe the steps necessary for secure installation, generation, and start-up of the system. The installation, generation, and start-up procedures may provide detailed information about the following:

- Changing the installation specific security characteristics of entities under the control of the security function
- Handling exceptions and problems
- Minimum system requirements for secure installation if applicable

In order to confirm that the installation, generation, and start-up procedures result in a secure configuration, the FAA evaluator may follow the developer's procedures and may perform the activities that customers are usually expected to perform to install, generate, and start-up the system (if applicable to the system), using the supplied guidance documentation only.

B.5 Development

The purpose of the development activity is to assess the design documentation in terms of its adequacy to understand how the system provides the security functions. This understanding is achieved through examination of descriptions of the security function design documentation. Design documentation consists of a functional specification (which describes the external interfaces of the system) and a high-level design (which describes the architecture of the system in terms of internal subsystems).

B.5.1 Functional Specification

The FAA evaluator examines the functional specification to determine that it contains all necessary informal[7] explanatory text. The informal functional specification comprises a

---

7 "Informal" refers to prose written in natural language. Informal writing is not subject to any notational or special restrictions other than those required as ordinary conventions for that language (e.g., grammar and

description of the security functions and a description of the externally-visible interfaces to the security function. For example, if an operating system presents the user with a means of self-identification, of creating files, of modifying or deleting files, of setting permissions defining what other users may access files, and of communicating with remote machines, its functional specification would contain descriptions of each of these functions. If there are also audit functions that detect and record the occurrences of such events, descriptions of these audit functions would also be expected to be part of the functional specification; while these functions are technically not directly invoked by the user at the external interface, they certainly are affected by what occurs at the user's external interface.

The FAA evaluator examines the functional specification to determine that it is internally consistent. The FAA evaluator validates the functional specification by ensuring that the descriptions of the interfaces making up the system security function interface are consistent with the descriptions of the security functions.

The FAA evaluator examines the functional specification to determine that it identifies all of the external system security function interfaces. The term "external" refers to that which is visible to the user. External interfaces to the system are either direct interfaces to the security function or interfaces to non-security function portions of the system that might have eventual access to the security function. These external interfaces that directly or indirectly access the security functions collectively make up the system security function interface.

It should be noted that all security functions reflected in the security functional requirements will have some sort of externally-visible manifestation. While not all of these are necessarily interfaces from which the security function can be tested, they are all externally-visible to some extent and must therefore be included in the functional specification.

The FAA evaluator examines the functional specification to determine that it describes all of the external Target of Evaluation (TOE) security function interfaces. All external interfaces are described in the functional specification, but only to the extent that the effect of each is made clear: interfaces to the security functions are completely described, while other interfaces are described only to the extent that it is clear that the security function is inaccessible through the interface. Because each external interface is a potential security

---

syntax). While no notational restrictions apply, the informal specification is also required to provide defined meanings for terms that are used in a context other than that accepted by normal usage. In contrast, semiformal writing follows in a restricted syntax language and formal writing employs a notation based upon well-established mathematical concepts used to define the syntax and semantics of the notation and the proof rules that support logical reasoning. Formal and semiformal writing are typically accompanied by supporting explanatory (informal) prose.

function interface, the functional specification must contain a description of each interface in sufficient detail so that the FAA evaluator can determine whether the interface is security relevant.

Some architectures lend themselves to readily provide this interface description in sufficient detail for groups of external interfaces. For example, a kernel architecture is such that all calls to the operating system are handled by kernel programs; any calls that might violate the security policy must be called by a program with the privilege to do so. All programs that execute with privilege must be included in the functional specification. Any program external to the kernel that executes without privilege is incapable of affecting the security policy and may, therefore, be excluded from the functional specification. It is worth noting that, while the FAA evaluator's understanding of the interface description can be expedited in cases where there is a kernel architecture, such an architecture is not necessary.

The FAA evaluator examines the presentation of the security function interface to determine that it adequately and correctly describes the behavior of the system at each external interface describing effects, exceptions and error messages. In order to assess the adequacy and correctness of an interface's presentation, the evaluator uses the functional specification, the system summary specification, and the user and administrator guidance to assess the following factors:

- All security relevant user input parameters (or a characterization of those parameters) should be identified. For completeness, parameters outside of direct user control should be identified if they are usable by administrators.
- All security relevant behavior described in the reviewed guidance should be reflected in the description of semantics in the functional specification. This should include an identification of the behavior in terms of events and the effect of each event. For example, if an operating system provides a rich file system interface, where it provides a different error code for each reason why a file is not opened upon request (e.g., access denied, no such file, file is in use by another user, user is not authorized to open the file after 5 pm), the functional specification should explain that a file is either opened upon request, or else that an error code is returned. (While the functional specification may enumerate all these different reasons for errors, it need not provide such detail.) The description of the semantics should include how the security requirements apply to the interface (e.g., whether the use of the interface is an auditable event and, if so, the information that can be recorded).
- All interfaces are described for all possible modes of operation. If the security function provides the notion of privilege, the description of the interface should explain how the interface behaves in the presence or absence of privilege.
- The information contained in the descriptions of the security relevant parameters and syntax of the interface should be consistent across all documentation.

Verification of the above is done by reviewing the functional specification and the system summary specification, as well as the user and administrator guidance provided by the developer. For example, if the system were an operating system and its underlying hardware, the evaluator would look for discussions of user-accessible programs, descriptions of protocols used to direct the activities of programs, descriptions of user-accessible databases used to direct the activities of programs, and for user interfaces (e.g., commands, application program interfaces) as applicable to the system under evaluation; the evaluator would also ensure that the processor instruction set is described. This review might be iterative, such that the FAA evaluator would not discover the functional specification to be incomplete until the design, source code, or other evidence is examined and found to contain parameters or error messages that have been omitted from the functional specification.

The FAA evaluator examines the functional specification to determine that the security function is fully represented. In order to assess the completeness of the security function representation, the FAA evaluator consults the system summary specification, the user guidance, and the administrator guidance. None of these should describe security functions that are absent from the security function presentation of the functional specification.

B.5.2 High-Level Design

The objective of this activity is to determine whether the high-level design provides a description of the security function in terms of major structural units (i.e., subsystems), and is a correct realization of the functional specification.

An informal high-level design is expressed in terms of sequences of actions that occur in each subsystem in response to stimulus at its interface. For example, a firewall might be composed of subsystems that deal with packet filtering, with remote administration, and with auditing. The high-level design description of the firewall would describe the actions that are taken, in terms of what actions each subsystem takes when an incoming packet arrives at the firewall.

The FAA evaluator examines the presentation of the high-level design to determine that it is internally consistent. The FAA evaluator examines the high-level design to determine that the security function is described in terms of subsystems. With respect to the high-level design, the term subsystem refers to large, related units (such as memory-management, file-management, process-management). Breaking a design into the basic functional areas aids in the understanding of the design.

The primary purpose for examining the high-level design is to aid the FAA evaluator understanding of the system. The developer's choice of subsystem definition, and of the grouping of security functions within each subsystem, are an important aspect of making the high-level design useful in understanding the system's intended operation. The FAA evaluator makes an assessment as to the appropriateness of the number of subsystems presented by the developer, and also of the choice of grouping of functions within

subsystems. The evaluator should ensure that the decomposition of the security function into subsystems is sufficient to gain a high-level understanding of how the functionality of the security function is provided. The subsystems used to describe the high-level design need not be called "subsystems," but should represent a similar level of decomposition. For example, the design may be decomposed using "layers" or "managers." The FAA evaluator validates the subsystem interface specifications by ensuring that the interface specifications are consistent with the description of the purpose of the subsystem.

The FAA evaluator examines the high-level design to determine that it describes the security functionality of each subsystem. The security functional behavior of a subsystem is a description of what the subsystem does. This should include a description of any actions that the subsystem may be directed to perform through its functions and the effects the subsystem may have on the security state of the system (e.g., changes in subjects, objects, security databases).

The FAA evaluator checks the high-level design to determine that it identifies all hardware, firmware, and software required by the security function. The FAA evaluator examines the high-level design to determine that it includes a presentation of the functions provided by the supporting protection mechanisms implemented in the underlying hardware, firmware, or software. The FAA evaluator checks that the high-level design identifies which of the interfaces to the subsystems of the security function are externally visible.

B.6 Guidance Documents

The purpose of the guidance document activity is to judge the adequacy of the documentation describing how to use the operational system. Such documentation includes both that aimed at trusted administrators and non-administrator users whose incorrect actions could adversely affect the security of the system, as well as that aimed at untrusted users whose incorrect actions could adversely affect the security of their own data.

B.6.1 Security Administrator Guidance

The FAA evaluator examines the administrator guidance to determine that it describes the administrative security functions and interfaces available to the administrator of the system. The term administrator is used to indicate a human user who is trusted to perform security critical operations within the system, such as setting system configuration parameters. The operations may affect the enforcement of the security function, and the administrator therefore possesses specific privileges necessary to perform those operations. The role of the administrator(s) has to be clearly distinguished from the role of non-administrative users of the system. There may be different administrator roles or groups defined that are recognized by the system and that can interact with the security function such as auditor, administrator, or daily-management. Each role can encompass an extensive set of capabilities, or can be a single one. The capabilities of these roles and their associated

privileges should be described. Different administrator roles and groups should be taken into consideration by the administrator guidance. The administrator guidance should contain an overview of the security functionality that is visible at the administrator interfaces. The administrator guidance should identify and describe the purpose, behavior, and interrelationships of the administrator security interfaces and functions. For each administrator security interface and function, the administrator guidance should:

- Describe the method(s) by which the interface is invoked (e.g., command-line, programming-language system calls, menu selection, command button).
- Describe the parameters to be set by the administrator, their valid and default values.
- Describe the immediate security function response, message, or code returned.

The FAA evaluator examines the administrator guidance to determine that it describes how to administer the system in a secure manner. The administrator guidance describes how to operate the system according to the security policy in an IT environment that is consistent with the one specified for the system use.

The FAA evaluator examines the administrator guidance to determine that it contains warnings about functions and privileges that should be controlled in a secure processing environment. The configuration of the system may allow users to have dissimilar privileges to make use of the different functions of the system. This means that some users may be authorized to perform certain functions while other users may not be so authorized. These functions and privileges should be described by the administrator guidance. The administrator guidance identifies the functions and privileges that must be controlled, the types of controls required for them, and the reasons for such controls. Warnings address expected effects, possible side effects, and possible interactions with other functions and privileges.

The FAA evaluator examines the administrator guidance to determine that it describes all assumptions regarding user behavior that are relevant to the secure operation of the system. Assumptions about the user behavior may be described in more detail in the statement of the system security environment. However, only the information that is of concern to the secure operation of the system need be included in the administrator guidance. An example of a user's responsibility necessary for secure operation is that users will keep their passwords secret.

The FAA evaluator examines the administrator guidance to determine that it describes all security parameters under the control of the administrator indicating secure values as appropriate. For each security parameter, the administrator guidance should describe the purpose of the parameter, the valid and default values of the parameter, and secure and insecure use settings of such parameters, both individually and in combination.

The FAA evaluator examines the administrator guidance to determine that it describes each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the security function. All types of security-relevant events are detailed, such that an administrator knows what events may occur and what action (if any) the administrator may have to take in order to maintain security. Security-relevant events that may occur during operation of the system (e.g., audit trail overflow, system crash, updates to user records, such as when a user account is removed when the user leaves the organization) are adequately defined to allow administrator intervention to maintain secure operation.

The FAA evaluator examines the administrator guidance to determine that it is consistent with all other documents supplied. The FAA evaluator examines the administrator guidance to determine that it describes all IT security requirements for the IT environment, if any, of the system that are relevant to the administrator.

B.6.2 User Guidance

The objectives of this activity are to determine whether the user guidance describes the security functions and interfaces provided by the security function and whether this guidance provides instructions and guidelines for the secure use of the system.

The FAA evaluator examines the user guidance to determine that it describes the security functions and interfaces available to the non-administrative users of the system. The user guidance should contain an overview of the security functionality that is visible at the user interfaces. The user guidance should identify and describe the purpose of the security interfaces and functions.

The FAA evaluator examines the user guidance to determine that it describes the use of user-accessible security functions provided by the system. The user guidance should identify and describe the behavior and interrelationship of the security interfaces and functions available to the user. If the user is allowed to invoke a system security function, the user guidance provides a description of the interfaces available to the user for that function. For each interface and function, the user guidance should:

- Describe the method(s) by which the interface is invoked (e.g., command-line, programming-language system call, menu selection, command button).
- Describe the parameters to be set by the user and their valid and default values.
- Describe the immediate security function response, message, or code returned.

The FAA evaluator examines the user guidance to determine that it contains warnings about user-accessible functions and privileges that should be controlled in a secure processing environment. The configuration of the system may allow users to have dissimilar privileges in making use of the different functions of the system. This means that some users

are authorized to perform certain functions, while other users may not be so authorized. The user guidance should identify the functions and privileges that can be used, the types of commands required for them, and the reasons for such commands. The user guidance should contain warnings regarding the use of the functions and privileges that must be controlled. Warnings should address expected effects, possible side effects, and possible interactions with other functions and privileges.

The FAA evaluator examines the user guidance to determine that it presents all user responsibilities necessary for secure operation of the system, including those related to assumptions regarding user behavior found in the statement of system security environment. Assumptions about the user behavior may be described in more detail in the statement of the TOE security environment. However, only the information that is of concern to the secure operation of the system need be included in the user guidance. The user guidance should provide advice regarding effective use of the security functions (e.g., reviewing password composition practices, suggested frequency of user file backups, discussion on the effects of changing user access privileges). An example of a user's responsibility necessary for secure operation is that users will keep their passwords secret. The user guidance should indicate whether the user can invoke a function or whether the user requires the assistance of an administrator.

The FAA evaluator examines the user guidance to determine that it is consistent with all other documentation supplied. The FAA evaluator ensures that the user guidance and all other documents supplied for evaluation do not contradict each other. The FAA evaluator examines the user guidance to determine that it describes all security requirements for the IT environment of the system that are relevant to the user.

B.7 Developer and FAA Testing

The purpose of this activity is to determine, by independently testing a subset of the security function, whether the system behaves as specified in the design documentation and in accordance with the system security functional requirements and security policy.

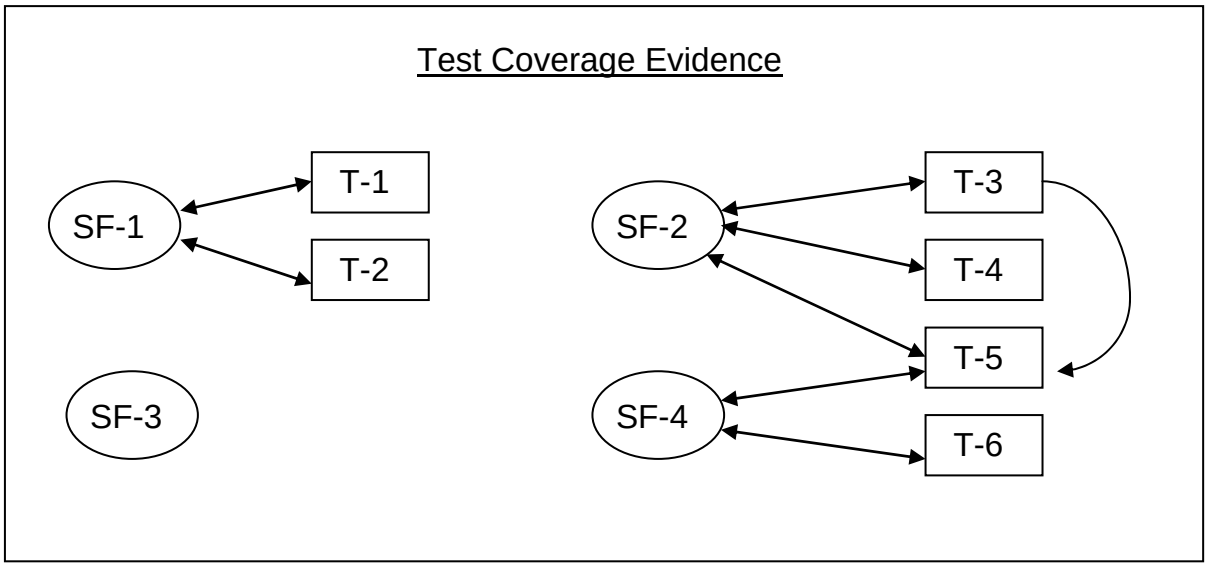
The FAA evaluator analyses the developer's tests to determine the extent to which they are sufficient to demonstrate that security functions perform as specified, and to understand the developer's approach to testing. The FAA evaluator also executes a subset of the developer's tests as documented to gain confidence in the developer's test results. The FAA evaluator will use the results of this analysis as an input to independently testing a subset of the security function. With respect to this subset, the FAA evaluator tests take a testing approach that is different from that of the developer's tests, particularly if the developer's tests have shortcomings. One such factor affecting the composition of the subset is known public domain weaknesses (e.g., those published by activities such CERT and bugtraq). To determine the adequacy of developer's test documentation or to create new tests, the FAA evaluator needs to understand the desired expected behavior of a security function in the

context of the requirements it is to satisfy. The FAA evaluator may choose to focus on one security function at a time, examining the requirement and the relevant parts of the functional specification and guidance documentation to gain an understanding of the way the system is expected to behave.

B.7.1 Analysis of Coverage

The coverage analysis provide by the developer is required to show the correspondence between the test provided as evaluation evidence and the functional specification. However, the coverage analysis need not demonstrate that all security functions have been tested, or that all external interfaces to the security function have been tested. Such shortcomings are considered by the FAA evaluator during the independent testing activity.

The FAA evaluator examines the test coverage evidence to determine that the correspondence between the tests identified in the test documentation and the functional specification is accurate. Correspondence may take the form of a table or matrix. The coverage evidence required for this component will reveal the extent of coverage, rather than to show complete coverage. In cases where coverage is shown to be poor the FAA evaluator should increase the level of independent testing to compensate. Figure B-1 displays a conceptual framework of the correspondence between security functions described in the functional specification and the tests outlined in the test documentation used to test them. Tests may involve one or multiple security functions depending on the test dependencies or the overall goal of the test being performed. The identification of the tests and the security functions presented in the test coverage evidence should be unambiguous, providing a clear correspondence between the identified tests and the functional specification of the security functions tested. In Figure B-1, SF-3 does not have tests attributed to it. Therefore, coverage with respect to the functional specification is incomplete. Incomplete coverage, however, will not impact the verdict of this activity as the coverage evidence does not have to show complete coverage of the security functions identified in the functional specification. Dependence of test-5 on test-3 is also illustrated.



Test documentation		Functional specification	
Test-1	**(T-1)**	**Security Function-1**	**(SF-1)**
Test-2	**(T-2)**	**Security Function-2**	**(SF-2)**
Test-3	**(T-3)**	**Security Function-3**	**(SF-3)**
Test-4	**(T-4)**	**Security Function-4**	**(SF-4)**
Test-5	**(T-5)**		
Test-6	**(T-6)**		

Figure B-1. Correspondence Between Security Functions and Tests

B.7.2 Analysis of Developer's Functional Tests

The objective of this activity is to determine whether the developer's functional test documentation is sufficient to demonstrate that security functions perform as specified. The FAA evaluator may wish to employ a sampling strategy when analyzing the developer's tests. For the developer tests provided, the FAA evaluator determines whether the tests are repeatable, and the extent to which the developer's tests can be used for the FAA evaluator's independent testing effort. Any security function for which the developer's test results indicate that it may not perform as specified should be tested independently by the FAA evaluator to determine whether or not it does.

The FAA evaluator checks that the test documentation includes test plans, test procedure descriptions, expected test results, and actual test results. The FAA evaluator checks that the test plan identifies the security functions to be tested. One method that could be used to identify the security function to be tested is a reference to the appropriate part(s) of the functional specification that specifies the particular security function.

The FAA evaluator examines the test plan to determine that it describes the goal of the tests performed. The test plan provides information about how the security functions are tested and the test configuration in which testing occurs.

The FAA evaluator examines the test plan to determine that the system test configuration is consistent with the configuration identified for evaluation. The system used for testing should have the same unique reference as established by the Configuration Management activity and the developer supplied test documentation. It is possible to specify more than one configuration for evaluation. The system may be composed of a number of distinct hardware and software implementations that need to be tested. The FAA evaluator verifies that there are test configurations consistent with each evaluated configuration described. The FAA evaluator should consider the assumptions about the security aspects of the system environment that may apply to the test environment. There may be some assumptions that do not apply to the test environment. For example, an assumption about user clearances may not apply. However, an assumption about a single point of connection to a network would apply.

The FAA evaluator examines the test plan to determine that it is consistent with the test procedure descriptions. The FAA evaluator checks that the test procedure descriptions identify each security function behavior to be tested. One method that may be used to identify the security function behavior to be tested is a reference to the appropriate part(s) of the design specification that specifies the particular behavior to be tested.

The FAA evaluator examines the test procedure descriptions to determine that sufficient instructions are provided to establish reproducible initial test conditions including ordering dependencies if any. Some steps may have to be performed to establish initial conditions. For example, user accounts need to be added before they can be deleted. An example of ordering dependencies on the results of other tests is the need to test the audit function before relying on it to produce audit records for another security mechanism such as access control. Another example of an ordering dependency would be where one test case generates a file of data to be used as input for another test case.

The FAA evaluator examines the test procedures to determine that instructions are provided for a reproducible, sufficient stimulation of the security functions and observation of their behavior. Stimulus is usually provided to a security function through the security function interface. Once a stimulus (input) is provided, the results at the security function interface are observed and analyzed. Note that it is not possible to always observe the function responses at the external interface, some things happen behind the interface. The test procedures must contain enough detail to unambiguously describe the stimulus and the expected behavior. Complex interactions at interfaces, such as extensive sequential protocol exchanges, are often stimulated by a simulator as part of the test equipment. For systems that are tested for their effect on other systems, both security function and non-security function interfaces are included in the stimulation, observation, and analysis. When the security

objectives include anomaly detection (e.g., unauthorized behavior by an authorized user or administrator or an imposter masquerading as an authorized user or administrator), the test procedures include negative tests and observation at all interfaces. For systems that are not tested for their effect on other systems through the non-security function interfaces, analysis can be limited to the security function of only that system.

The FAA evaluator examines the test documentation to determine that sufficient expected tests results are included. The expected test results are needed to determine whether or not a test has been successfully performed. Expected test results are sufficient if they are unambiguous and consistent with expected behavior given the testing approach.

The FAA evaluator checks that the expected test results in the test documentation are consistent with the actual test results provided. A comparison of the actual and expected test results provided by the developer will reveal any inconsistencies between the results. It may be that a direct comparison of actual results cannot be made until some data reduction or synthesis has been first performed. In such cases, the developer's test documentation should describe the process to reduce or synthesize the actual data. For example, the developer may need to test the contents of a message buffer after a network connection has occurred to determine the contents of the buffer. The message buffer will contain a binary number. This binary number would have to be converted to another form of data representation in order to make the test more meaningful. The conversion of this binary representation of data into a higher-level representation will have to be described by the developer in enough detail to allow the FAA evaluator to perform the conversion process (i.e., synchronous or asynchronous transmission, number of stop bits, parity).

It should be noted that the description of the process used to reduce or synthesize the actual data is used by the FAA evaluator not to actually perform the necessary modification but to assess whether this process is correct. It is up to the developer to transform the expected test results into a format that allows an easy comparison with the actual test results. If the expected and actual test results for any test are not the same, then a demonstration of the correct operation of a security function has not been achieved. Such an occurrence will influence the FAA evaluator's independent testing effort to include testing the implicated security function. The FAA evaluator also considers increasing the sample of evidence upon which this work unit is performed.

The FAA evaluator documents the analysis of the developer testing effort, outlining the testing approach, configuration, depth and results. The developer testing information recorded in the FAA documentation allows the FAA evaluator to convey the overall testing approach and effort expended on the testing of the system by the developer. The intent of producing this information is to give a meaningful overview of the developer testing effort. It is not intended that the information regarding developer testing in the FAA documentation be an exact reproduction of specific test steps or results of individual tests. The intention is to provide enough detail to allow others to gain some insight about the developer's testing

approach, amount of testing performed, system test configurations, and the overall results of the developer testing. Information that would typically be found in the FAA documentation regarding the developer testing effort is:

- System test configurations. The particular configurations of the system that were tested.
- Testing approach. An account of the overall developer testing strategy employed.
- Amount of developer testing performed. A description on the extent of coverage and depth of developer testing.
- Testing results. A description of the overall developer testing results.

This list is by no means exhaustive and is only intended to provide some context as to the type of information that should be present in the FAA documentation concerning the developer testing effort.

B.7.3 Independent Testing

The purpose of independent testing is to determine, by independently testing a subset of the security function, whether the system behaves as specified, and to gain confidence in the developer's test results by performing a sample of the developer's tests. As addressed in Section 2, independent testing is a joint responsibility of the FAA Security Testing (Evaluation) Organization (ACB), and the ISS Policy and Guidance Organization (AIS).

The FAA evaluator examines the system to determine that the test configuration is consistent with the configuration under evaluation. The system used for testing should have the same unique reference as established by the Configuration Management activity and the developer supplied test documentation. It is possible to specify more than one configuration for evaluation. The system may be composed of a number of distinct hardware and software implementations that need to be tested. The FAA evaluator verifies that there are test configurations consistent with each evaluated configuration. The FAA evaluator considers the assumptions about the security aspects of the system environment that may apply to the test environment. There may be some assumptions that do not apply to the test environment. For example, an assumption about user clearances may not apply. However, an assumption about a single point of connection to a network would apply. If any test resources are used (e.g., meters, analyzers) it will be the FAA evaluator's responsibility to ensure that these resources are calibrated correctly.

The FAA evaluator examines the test system to determine that it has been installed properly and is in a known state. The FAA evaluator examines the set of resources provided by the developer or otherwise available for testing to determine that they are equivalent to the set of resources used by the developer to functionally test the security function. The resource set may include laboratory access and special test equipment, among others.

Resources that are not identical to those used by the developer need to be equivalent in terms of any impact they may have on test results.

The FAA evaluator devises a test subset. The FAA evaluator selects a test subset and testing strategy that is appropriate for the system. One extreme testing strategy would be to have the test subset contain as many security functions as possible tested with little rigor. Another testing strategy would be to have the test subset contain a few security functions based on their perceived relevance and rigorously test these functions. Typically the testing approach taken by the FAA evaluator should fall somewhere between these two extremes. The FAA evaluator should exercise most of the security functional requirements using at least one test, but testing need not demonstrate exhaustive specification testing. The FAA evaluator, when selecting the subset of the security function to be tested, should consider the following factors:

- The developer test evidence. The developer test evidence consists of: the test coverage analysis, and the test documentation. The developer test evidence will provide insight as to how the security functions have been exercised by the developer during testing. The evaluator applies this information when developing new tests to independently test the system. Specifically the evaluator should consider:
  - Augmentation of developer testing for specific security function(s). The FAA evaluator may wish to perform more of the same type of tests by varying parameters to more rigorously test the security function.
  - Supplementation of developer testing strategy for specific security function(s). The FAA evaluator may wish to vary the testing approach of a specific security function by testing it using another test strategy.
- The number of security functions from which to draw upon for the test subset. Where the system includes only a small number of security functions, it may be practical to rigorously test all of the security functions. For systems with a large number of security functions this will not be cost-effective, and sampling is required.
- Maintaining a balance of evaluation activities. The effort expended on the independent test activity should be commensurate with that expended on any other test and evaluation activity. The level of coverage provided will be a significant factor in determining the appropriate effort expended by the FAA evaluator.

The FAA evaluator selects the security functions to compose the subset. This selection will depend on a number of factors, and consideration of these factors may also influence the choice of test subset size:

- Rigor of developer testing of the security functions. Some security functions identified in the functional specification may have had little or no developer test

evidence attributed to them. Those security functions that the FAA evaluator determines require additional testing should be included in the test subset.

- Developer test results. If the results of developer tests cause the FAA evaluator to doubt that a security function, or aspect thereof, operates as specified, then the FAA evaluator should include such security functions in the test subset.
- Known public domain weaknesses commonly associated with the type of system (e.g., operating system, firewall). Know public domain weaknesses associated with the type of system will influence the selection process of the test subset. The FAA evaluator should include those security functions that address known public domain weaknesses for that type of system in the subset (know public domain weaknesses in this context does not refer to vulnerabilities as such but to inadequacies or problem areas that have been experienced with this particular type of system). If no such weaknesses are known, then a more general approach of selecting a broad range of security functions may be more appropriate.
- Significance of security functions. Those security functions more significant than others in terms of the security objectives for the system should be included in the test subset.
- Strength of function claims. All security functions for which a specific strength of function claim has been made should be included in the test subset.
- Complexity of the security function. Complex security functions may require complex tests that impose onerous requirements on the developer or the FAA evaluator, which will not be conducive to cost-effective evaluations. Conversely, complex security functions are a likely area to find errors and are good candidates for the subset. The FAA evaluator will need to strike a balance between these considerations.
- Implicit testing. Testing some security functions may often implicitly test other security functions, and their inclusion in the subset may maximize the number of security functions tested (albeit implicitly). Certain interfaces will typically be used to provide a variety of security functionality, and will tend to be the target of an effective testing approach.
- Types of interfaces to the system (e.g., programmatic, command-line, protocol). The FAA evaluator considers including tests for all different types of interfaces that the system supports.
- Functions that are innovative or unusual. Where the system contains innovative or unusual security functions, which may feature strongly in marketing literature, these should be strong candidates for testing.

This guidance articulates factors to consider during the selection process of an appropriate test subset, but these are by no means exhaustive.

The FAA evaluator produces test documentation for the test subset that is sufficiently detailed to enable the tests to be reproducible. With an understanding of the expected behavior of a security function, the FAA evaluator has to determine the most feasible way to test the function. Specifically the FAA evaluator considers:

- The approach that will be used, for instance, whether the security function will be tested at an external interface, at an internal interface using a test harness, or will an alternate test approach be employed (e.g., in exceptional circumstances, a code inspection.
- The security function interface(s) that will be used to stimulate the security function and observe responses.
- The initial conditions that will need to exist for the test (i.e., any particular objects or subjects that will need to exist and security attributes they will need to have).
- Special test equipment that will be required to either stimulate a security function (e.g., packet generators) or make observations of a security function (e.g., network analyzers).

The FAA evaluator may find it practical to test each security function using a series of test cases, where each test case will test a very specific aspect of expected behavior. The FAA evaluator test documentation should specify the derivation of each test, tracing it back to the relevant design specification.

The FAA evaluator conducts testing. The FAA evaluator uses the test documentation developed as a basis for executing tests on the system. The test documentation is used as a basis for testing but this does not preclude the FAA evaluator from performing additional ad hoc tests. The FAA evaluator may devise new tests based on behavior of the system discovered during testing. These new tests are recorded in the test documentation.

The FAA evaluator records the following information about the tests that compose the test subset:

- Identification of the security function behavior to be tested.
- Instructions to connect and setup all required test equipment as required to conduct the test.
- Instructions to establish all prerequisite test conditions.
- Instructions to stimulate the security function.
- Instructions for observing the behavior of the security function.

- Descriptions of all expected results and the necessary analysis to be performed on the observed behavior for comparison against expected results.
- Instructions to conclude the test and establish the necessary post-test state for the system.
- Actual test results.

The level of detail should be such that another person could repeat the tests and obtain an equivalent result. While some specific details of the test results may be different (e.g., time and date fields in an audit record) the overall result should be identical. There may be instances when it is unnecessary to provide all the information presented in this work unit (e.g., the actual test results of a test may not require any analysis before a comparison between the expected results can be made). The determination to omit this information is left to the FAA evaluator, as is the justification.

The FAA evaluator checks that all actual test results are consistent with the expected test results. Any differences in the actual and expected test results may indicate that the system does not perform as specified or that the FAA evaluator test documentation may be incorrect. Unexpected actual results may require corrective maintenance to the system or test documentation and perhaps require re-running of impacted tests and modifying the test sample size and composition. This determination is left to the FAA evaluator, as is its justification.

The FAA evaluator conducts testing using a sample of tests found in the developer test plan and procedures. The overall aim of this work unit is to perform a sufficient number of the developer tests to confirm the validity of the developer's test results. The FAA evaluator has to decide on the size of the sample, and the developer tests that will compose the sample. Taking into consideration the overall evaluator effort for the entire tests activity, normally 20% of the developer's tests should be performed although this may vary according to the nature of the system, and the test evidence supplied. All the developer tests can be traced back to specific security function(s). Additionally, the evaluator may wish to employ a random sampling method to select developer tests to include in the sample.

The FAA evaluator checks that all the actual test results are consistent with the expected test results. Inconsistencies between the developer's expected test results and actual test results will compel the FAA evaluator to resolve the discrepancies. Inconsistencies encountered by the FAA evaluator could be resolved by a valid explanation and resolution of the inconsistencies by the developer. If a satisfactory explanation or resolution can not be reached, the FAA evaluator's confidence in the developer's test results may be lessened and it may even be necessary for the FAA evaluator to increase the sample size, to regain confidence in the developer testing. If the increase in sample size does not satisfy the FAA evaluator's concerns, it may be necessary to repeat the entire set of developer's tests.

Ultimately, deficiencies with the developer's tests need to result in either corrective action to the developer's tests or in the production of new tests by the FAA evaluator.

The FAA evaluator documents the FAA testing effort, outlining the testing approach, configuration, depth and results. The FAA testing information reported in the documentation allows the FAA evaluator to convey the overall testing approach and effort expended on the testing activity. The intent of providing this information is to give a meaningful overview of the testing effort. It is not intended that the information regarding testing in the documentation be an exact reproduction of specific test instructions or results of individual tests. The intention is to provide enough detail to allow other people to gain some insight about the testing approach chosen, amount of FAA evaluator testing performed, amount of developer tests performed, system test configurations, and the overall results of the testing activity. Information that would typically be found in the documentation regarding the evaluator testing effort is:

- System test configurations. The particular configurations of the system that were tested.
- Subset size chosen. The amount of security functions that were tested during the evaluation and a justification for the size.
- Selection criteria for the security functions that compose the subset. Brief statements about the factors considered when selecting security functions for inclusion in the subset.
- Security functions tested. A brief listing of the security functions that merited inclusion in the subset.
- Developer tests performed. The amount of developer tests performed and a brief description of the criteria used to select the tests.
- Verdict for the activity. The overall judgment on the results of testing during the evaluation.

This list is by no means exhaustive and is only intended to provide some context as to the type of information that should be present in the documentation concerning the testing the FAA evaluator performed during the evaluation.

B.8 Vulnerability Assessment

The purpose of the vulnerability assessment activity is to determine the exploitability of flaws or weaknesses in the system in the intended environment. This determination is based upon analysis performed by the developer, and may be supported by FAA penetration testing.

B.8.1 Strength of Security Functions

The objectives of this activity are to determine whether Strength of Security Functions claims are made for all probabilistic or permutational mechanisms (e.g., a password or hash function) and whether the developer's Strength of Security Functions claims are supported by an analysis that is correct.

Strength of Security Functions analysis is performed on mechanisms that are probabilistic or permutational in nature, such as password mechanisms or biometrics. Where more than one probabilistic or permutational mechanism is employed to provide a security function, each distinct mechanism must be analyzed. The manner in which these mechanisms combine to provide a security function will determine the overall Strength of Security Functions level for that function. The FAA evaluator needs design information to understand how the mechanisms work together to provide a function, and a minimum level for such information is given by the High-Level Design. The available information should be used to support the evaluator's analysis when required.

The FAA evaluator checks that the developer has provided a Strength of Security Functions analysis for each security mechanism for which there is a Strength of Security Functions claim.

The FAA evaluator examines the Strength of Security Functions analysis to determine that any assertions or assumptions supporting the analysis are valid. For example, it may be a flawed assumption that a particular implementation of a pseudo-random number generator will possess the required entropy necessary to seed the security mechanism to which the Strength of Security Functions analysis is relevant. Assumptions supporting the Strength of Security Functions analysis should reflect the worst case, unless worst case is explicitly invalidated by the claim. Where a number of different possible scenarios exist, and these are dependent on the behavior of the human user or attacker, the case that represents the lowest strength should be assumed unless, as previously stated, this case is invalid. For example, a strength claim based upon a maximum theoretical password space (i.e., all printable ASCII characters) would not be worst case because it is human behavior to use natural language passwords, effectively reducing the password space and associated strength. However, such an assumption could be appropriate if the system used IT measures, such as password filters to minimize the use of natural language passwords.

The FAA evaluator examines the Strength of Security Functions analysis to determine that any algorithms, principles, properties and calculations supporting the analysis are correct. The nature of this work unit is highly dependent upon the type of mechanism being considered. For example, Strength of Security Functions analysis for an identification and authentication function that is implemented using a password mechanism considers the maximum password space to ultimately arrive at a Strength of Security Functions rating. For biometrics, the analysis should consider resolution and other factors impacting the

mechanism's susceptibility to spoofing. Strength of Security Functions expressed as a rating is based on the minimum attack potential required to defeat the security mechanism.

The FAA evaluator examines the Strength of Security Functions analysis to determine that each Strength of Security Functions claim is met or exceeded. The FAA evaluator examines the Strength of Security Functions analysis to determine that all functions with a Strength of Security Functions claim meet the minimum strength level defined.

The FAA evaluator examines the Strength of Security Functions claims to determine that they are correct. Where the Strength of Security Functions analysis includes assertions or assumptions (e.g., about how many authentication attempts are possible per minute), the FAA evaluator independently confirms that these are correct. This may be achieved through testing or through independent analysis.

B.8.2 Developer Vulnerability Analysis

The objective of this activity is to determine whether the system, in its intended environment, has exploitable obvious vulnerabilities. Vulnerabilities may be in the public domain, or not, and may require skill to exploit, or not. These two aspects are related, but are distinct. It should not be assumed that, simply because a vulnerability is in the public domain, it can be easily exploited.

The following terms are used with the given specific meaning:

- Vulnerability - A weakness in the system that can be used to violate a security policy in some environment.
- Vulnerability analysis - A systematic search for vulnerabilities in the system, and an assessment of those found to determine their relevance for the intended environment for the system.
- Obvious vulnerability - A vulnerability that is open to exploitation that requires a minimum of understanding of the system, technical sophistication and resources.
- Potential vulnerability - A vulnerability the existence of which is suspected (by virtue of a postulated attack path), but not confirmed, in the system.
- Exploitable vulnerability - A vulnerability that can be exploited in the intended environment for the system.
- Non-exploitable vulnerability - A vulnerability that cannot be exploited in the intended environment for the system.
- Residual vulnerability - A non-exploitable vulnerability that could be exploited by an attacker with greater attack potential than is anticipated in the intended environment for the system.

- Penetration testing - Testing carried out to determine the exploitability of identified system potential vulnerabilities in the intended environment for the system.

The FAA evaluator examines the developer's vulnerability analysis to determine that the search for obvious vulnerabilities has considered all relevant information. The developer's vulnerability analysis should cover the developer's search for obvious vulnerabilities in at least all deliverables and public domain information sources. The FAA evaluator should use the evaluation deliverables as a basis for assessing the developer's search for obvious vulnerabilities.

The FAA evaluator examines the developer's vulnerability analysis to determine that each obvious vulnerability is described and that a rationale is given for why it is not exploitable in the intended environment for the system. The developer is expected to search for obvious vulnerabilities, based on knowledge of the system, and of public domain information sources. Given the requirement to identify only obvious vulnerabilities, a detailed analysis is not expected. The developer filters this information, based on the above definition, and shows that obvious vulnerabilities are not exploitable in the intended environment. The FAA evaluator needs to be concerned with three aspects of the developer's analysis:

- Whether the developer's analysis has considered all evaluation deliverables.
- Whether appropriate measures are in place to prevent the exploitation of obvious vulnerabilities in the intended environment.
- Whether some obvious vulnerabilities remain unidentified.

The FAA evaluator should not be concerned over whether identified vulnerabilities are obvious or not, unless this is used by the developer as a basis for determining non-exploitability. In such a case the FAA evaluator validates the assertion by determining resistance to an attacker with low attack potential for the identified vulnerability. The concept of obvious vulnerabilities is not related to that of attack potential. The latter is determined by the FAA evaluator during independent vulnerability analysis. The FAA evaluator may discover potential vulnerabilities during the evaluation, and the determination of how these should be addressed will be made by reference to the definition of obvious vulnerabilities and the concept of low attack potential. The determination as to whether some obvious vulnerabilities remain unidentified is limited to assessment of the validity of the developer's analysis, a comparison with available public domain vulnerability information, and a comparison with any further vulnerabilities identified by the FAA evaluator during the course of other evaluation activities.

A vulnerability is termed non-exploitable if one or more of the following conditions exist:

- Security functions or measures in the (IT or non-IT) environment prevent exploitation of the vulnerability in the intended environment. For instance, restricting physical access to the system to authorized users only may effectively render a system's vulnerability to tampering unexploitable.
- The vulnerability is exploitable but only by attackers possessing moderate or high attack potential. For instance, a vulnerability of a distributed system to session hijack attacks requires an attack potential beyond that required to exploit an obvious vulnerability. However, such vulnerabilities are reported in the documentation as residual vulnerabilities.
- Either the threat is not claimed to be countered or the violable organizational security policy is not claimed to be achieved. For instance, a firewall that makes no availability policy claim and is vulnerable to Transmission Control Protocol (TCP) SYN attacks (an attack on a common Internet protocol that renders hosts incapable of servicing connection requests) should not fail this evaluator action on the basis of this vulnerability alone.

The FAA evaluator examines the developer's vulnerability analysis to determine that it is consistent with the requirements and this guidance. The developer's vulnerability analysis may address a vulnerability by suggesting specific configurations or settings for system functions. If such operating constraints are deemed to be effective, then all such configurations/settings should be adequately described in the guidance so that they may be employed by the consumer.

B.8.3 Penetration Testing

Penetration testing (pen test or PT), introduced in Section 3.4, is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The purpose of penetration testing is to identify vulnerabilities that not identified by any other methodology. MITRE recommends that the FAA establish a policy for penetration testing in FAA Systems that balances the risks and benefits and provides uniform procedures, rules of engagement, and identified level of management authorization required. Additional detail is in Appendix Section D.9.3. PT requires management approval of the PT plan and rules of engagement,

The FAA evaluator devises penetration tests, building on the developer vulnerability analysis. The FAA evaluator prepares for penetration testing:

- As necessary to attempt to disprove the developer's analysis in cases where the developer's rationale for why a vulnerability is unexploitable is suspect in the opinion of the evaluator.

- As necessary to determine the susceptibility of the TOE, in its intended environment, to an obvious vulnerability not considered by the developer.

The FAA evaluator should have access to current information regarding obvious public domain vulnerabilities that may not have been considered by the developer, and may also have identified potential vulnerabilities as a result of performing other evaluation activities. The evaluator is not expected to test for vulnerabilities (including those in the public domain) beyond those which are obvious. In some cases, however, it will be necessary to carry out a test before the exploitability can be determined. Where, as a result of evaluation expertise, the evaluator discovers a vulnerability that is beyond obvious, this is reported in the documentation as a residual vulnerability.

With an understanding of the suspected obvious vulnerability, the FAA evaluator determines the most feasible way to test for the system's susceptibility. Specifically the FAA evaluator considers:

- The security function interfaces that will be used to stimulate the security function and observe responses;.
- Initial conditions that will need to exist for the test (i.e., any particular objects or subjects that will need to exist and security attributes they will need to have).
- Special test equipment that will be required to either stimulate a security function or make observations of a security function (although it is unlikely that specialist equipment would be required to exploit an obvious vulnerability).

The FAA evaluator produces penetration test documentation for the tests that build upon the developer vulnerability analysis, in sufficient detail to enable the tests to be repeatable. The test documentation shall include:

- Identification of the obvious vulnerability the system is being tested for.
- Instructions to connect and setup all required test equipment as required to conduct the penetration test.
- Instructions to establish all penetration test prerequisite initial conditions.
- Instructions to stimulate the security function.
- Instructions for observing the behavior of the security function.
- Descriptions of all expected results and the necessary analysis to be performed on the observed behavior for comparison against expected results.
- Instructions to conclude the test and establish the necessary post-test state for the system.

The intent of specifying this level of detail in the test documentation is to allow another tester to repeat the tests and obtain an equivalent result. The FAA evaluator will probably find it practical to carry out penetration testing using a series of test cases, where each test case will test for a specific obvious vulnerability.

The FAA evaluator conducts penetration testing, building on the developer vulnerability analysis. The FAA evaluator uses the penetration test documentation as a basis for executing penetration tests on the system, but this does not preclude the FAA evaluator from performing additional ad hoc penetration tests. If required, the FAA evaluator may devise ad hoc tests as a result of information learned during penetration testing that, if performed by the FAA evaluator, are to be recorded in the penetration test documentation. Such tests may be required to follow up unexpected results or observations, or to investigate potential vulnerabilities suggested to the FAA evaluator during the pre-planned testing.

The FAA evaluator records the actual results of the penetration tests. While some specific details of the actual test results may be different from those expected (e.g., time and date fields in an audit record) the overall result should be identical. Any differences should be justified.

The FAA evaluator examines the results of all penetration testing and the conclusions of all vulnerability analysis to determine that the system, in its intended environment, has no exploitable obvious vulnerabilities. If the results reveal that the system has obvious vulnerabilities, exploitable in its intended environment, then further mitigation is required before the system can be placed in service.

The FAA evaluator documents the penetration testing effort, outlining the testing approach, configuration, depth and results. The documented penetration testing information allows the FAA evaluator to convey the overall penetration testing approach and effort expended on this activity. The intent of providing this information is to give a meaningful overview of the FAA evaluator's penetration testing effort. It is not intended that the information regarding penetration testing be an exact reproduction of specific test steps or results of individual penetration tests. The intention is to provide enough detail to allow other testers to gain some insight about the penetration testing approach chosen, amount of penetration testing performed, system test configurations, and the overall results of the penetration testing activity. Information that would typically be found in the documentation regarding evaluator penetration testing efforts is:

- System test configurations. The particular configurations of the system that were penetration tested.
- Security functions penetration tested. A brief listing of the security functions that were the focus of the penetration testing.
- Verdict for the activity. The overall judgment on the results of penetration testing.

This list is by no means exhaustive and is only intended to provide some context as to the type of information that should be present in the documentation concerning the penetration testing the FAA evaluator performed.

The evaluator shall document all exploitable vulnerabilities and residual vulnerabilities, detailing for each:

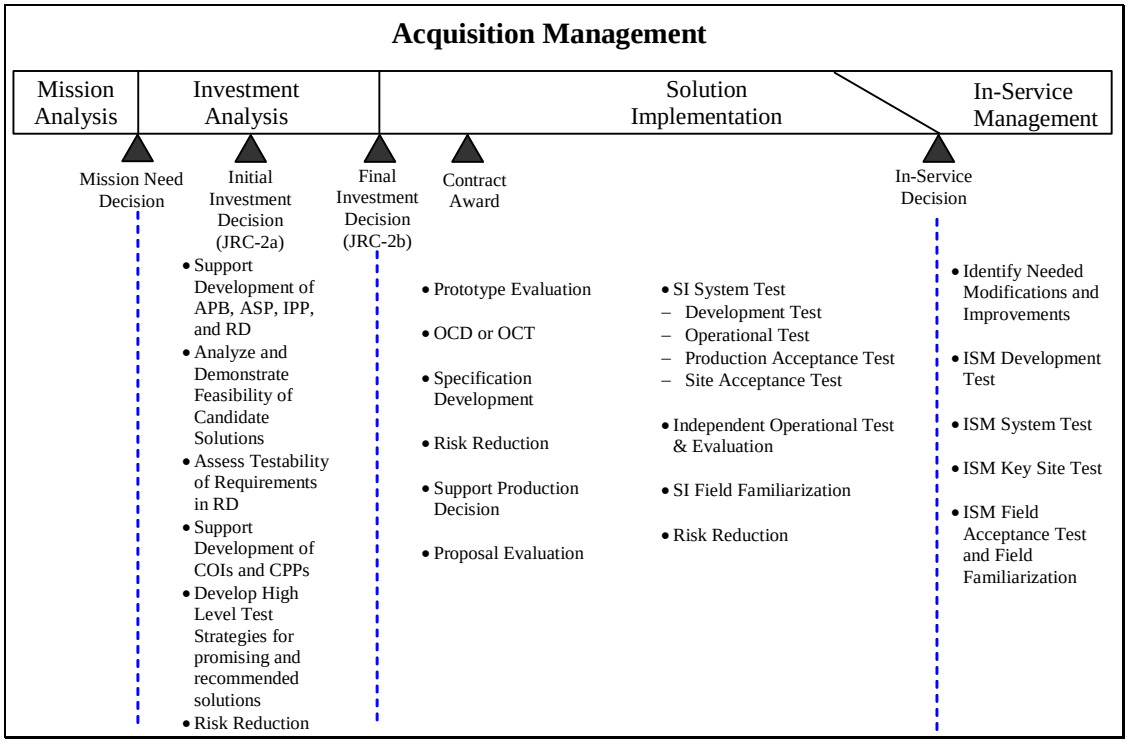
- Its source (e.g., CEM activity being undertaken when it was conceived, known to the evaluator, or read in a publication).
- The implicated security function(s), objective(s) not met, organizational security policy(ies) contravened and threat(s) realized.
- A description.
- Whether it is exploitable in its intended environment or not (i.e., exploitable or residual).
- Identification of evaluation party (e.g., developer, evaluator) who identified it.

Appendix C

Security Testing and the FAST[8]

C.1 Overview

The Test and Evaluation (T&E) processes for Acquisition Management have been developed to ensure consistency in testing approaches throughout the lifecycle of the program. Figure C-1 illustrates the relationship of test activities to the different phases of a typical acquisition. This overview section describes the relationship between these test activities, and explains how and when requirements are verified and how an assessment of system operational readiness is made.



APB	Acquisition Program Bulletin	OCD	Operational Capability Demonstration
ASP	Acquisition Strategy Paper	OCT	Operational Capability Test
IPP	Integrated Program Plan	RD	Requirements Document
ISM	In-Service Management	SI	Solution Implementation
JRC	Joint Resources Council		

Figure C-1. Tests and Test Activities Associated with NAS Acquisition Programs[9]

---

8 Based on *Acquisition Management System Test & Evaluation Process Guidelines*, April 2002.

9 *Op.cit.*, Figure 3-1.

The acquisition process begins with the Mission Analysis Phase, where a Mission Need Statement (MNS) is developed along with a set of initial requirements to support the determination of alternatives to be evaluated in the next phase. Test activities associated with the Mission Analysis Phase include concept feasibility demonstrations done to determine the viability of a concept or new capability, and an assessment of the testability of the initial requirements. A favorable outcome translates into a creation of a new Mission Need or an upgrade of an existing Mission Need, and an approved set of initial requirements and candidate alternatives. During the 2-part Investment Analysis Phase, which includes an initial and final investment analysis, the assessment of the testability of refined requirements and an estimation of the cost to conduct the test activities serves as input to the Final Requirements Document (FRD) and the Acquisition Program Baseline (APB) documents. Analysis and demonstration of the feasibility of candidate solutions may be conducted when appropriate to support the development and validation of the Requirements Document (RD). An Acquisition Strategy Paper (ASP) and Integrated Program Plan (IPP) are developed during this phase. The Investment Analysis Phase usually concludes with the authorization for the program to proceed to the Joint Resources Council (JRC) for a final investment decision. The JRC authorizes movement of the program to the Solution Implementation Phase.

Figure C-2 identifies the Test and Evaluation processes implemented during the Investment Analysis, Solution Implementation (SI) and In-Service Management (ISM) Phases of the Acquisition Management System (AMS). These processes also identify test process documentation, test tools and test environments that support the test objectives. The Test and Evaluation processes can be used to plan high-level T&E activities as they relate to the phases of the AMS.

The Solution Implementation (SI) Phase typically begins with refinement and expansion of the IPP leading to a full-scale development, Commercial-off-the-Shelf/Non-Developmental Item (COTS/NDI) procurement or Operational Prototype. SI System Test – which includes Development Tests (DTs), Operational Tests (OTs), Production Acceptance Tests (PATs) and Site Acceptance Tests (SATs); Independent Operational Test and Evaluation (IOT&E); and Field Familiarization are performed by various FAA organizations to verify that requirements have been met and that the system is ready for operational use. The Implementing Organization is responsible for system testing, the Office of Independent Operational Test and Evaluation (ATQ) is responsible for the IOT&E of designated programs, and site and regional Airway Facilities (AF) and Air Traffic (AT) personnel perform Field Familiarization for new systems. Early in the Solution Implementation Phase, prototype testing may be conducted to validate requirements and verify risk reduction plans associated with investment analysis assumptions. In some cases, the JRC may authorize the program to proceed through prototype testing but not to full-scale development until prototype test results are known and the JRC approves an updated APB.

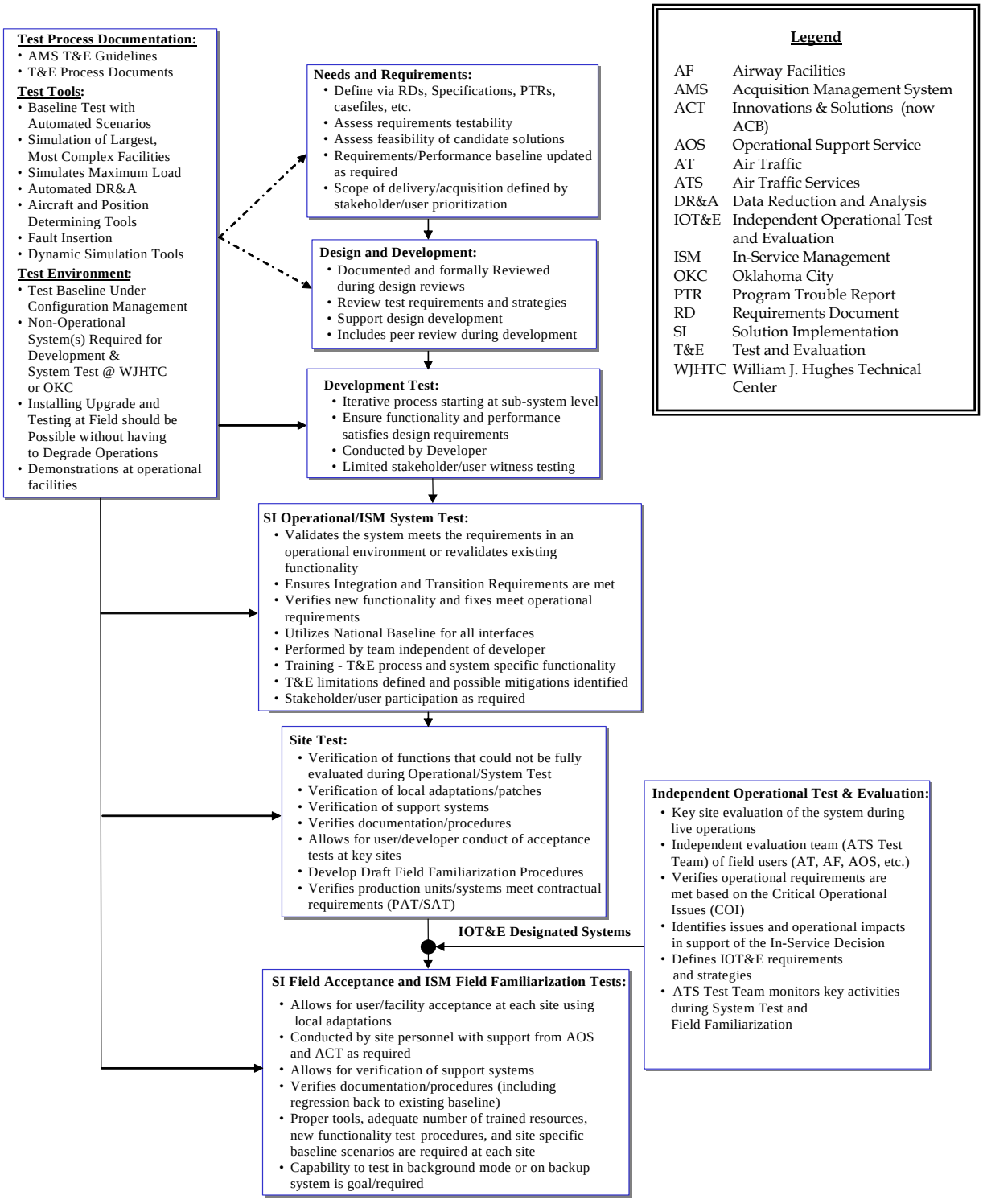


Figure C-2. Test and Evaluation Process[10]

10 *Op.cit.*, Figure 3-2.

System Tests are designed to accomplish two objectives during the Solution Implementation Phase. First, they verify satisfaction of all requirements associated with the acquisition of a system. Secondly, they answer the questions raised by the Critical Operational Issues (COIs) contained in the RD. When these tests are successfully completed, the Integrated Product Team (IPTs) or Business Service Organization (BSO) determines if the system is ready either for an In-Service Decision (ISD) (when IOT&E is not required), or to enter IOT&E. Following SAT, Field Familiarization is performed. Its primary objective is to verify that the site is ready to transition to the new system. IOT&E is performed on designated systems, as determined by the Associate Administrator for Air Traffic Services (ATS-1), and is designed to verify the operational readiness of the system in its intended operational environment. The IOT&E Report provides an operational readiness assessment to ATS-1 and the In-Service Decision authority.

The In-Service Management Phase typically starts after system deployment. Hardware/software (HW/SW) modification needs identified during the In-Service Management Phase of a system's lifecycle generally originate during the system's operation and sustainment. Changes to the baseline are handled via the National Airspace System (NAS) Change Proposal (NCP)/case file process. All HW/SW modifications performed during the In-Service Management (ISM) Phase of the acquisition management process must follow a structured, disciplined test, and evaluation process.

The process is accomplished through a six-phase approach that includes identification of needs and requirements, design and development, development test, ISM System Test (defined in paragraph 3.2.4.2 and not to be confused with SI System Test), Key Site Test, and Field Familiarization. T&E is conducted to validate that modified components, functionality, or enhancements operate properly and do not degrade system effectiveness or suitability. All activities are conducted with appropriate user/stakeholder involvement to ensure that the modifications are ready for deployment.

To make programs more efficient, it is sometimes necessary to tailor the standard acquisition/modification approach (e.g., Spiral Development, Tech Refresh, Prototyping, emergency hardware/software releases). Each In-Service Management Team must evaluate its test approach and tailor its processes for a specific program. Test standards detailed in this document should be used as a basis to develop a tailored test approach.

The FAA's T&E processes rely on the development and use of T&E documents, test tools, and test environments. These are utilized to confirm operational readiness by measuring specific system performance and simulating operational environments. Test documentation, test tools, and test environments are initially developed and used during SI T&E and are then modified and/or supplemented during ISM T&E based on changes/upgrades to the system.

C.1.1 Information Systems Security (ISS) Test and Evaluation

The objective of ST&E is to assess the technical implementation of the security design and to ascertain that security features have been properly implemented as documented. ST&E should also validate the proper integration and operation of all security features.

Individual tests are used to evaluate system conformance with the defined requirements, mission, environment, and architecture.

The ST&E test plan and procedures are developed to document the testing strategy. In reality, the ST&E test plan and procedures should also include tests against the security requirements stated in other documents such as the Protection Profile, System Level Specification (SLS), System Requirements Document (SRD), or System Specification Document (SSD).[11] These security requirements are typically based on an analysis of threats to the system. The ST&E test plan and procedures must be repeatable and used at various phases of a remediation process.

The scope of ST&E includes analysis and testing in the system's operational environment as well as the developmental or laboratory environment. The differences between the generic laboratory environment and the operational environment typically include the configuration of system parameters and local changes; especially local parameters and configuration settings. System interfaces, connectivity, and data flow must be tested. If the communication partner(s) is (are) not available to participate in the test configuration, then either simulation will be necessary or another means must be identified for verifying that the system performs the necessary security functions. For security testing, the simulation must include penetration attempts and other attacks on the security policy.

The philosophy and strategy that are used in ST&E are generally based on "Best" practices (or commonly used practices) that have been identified in the information security community. Sources used for best practices in ISS testing and evaluation include:

- *FAA Acquisition Management System Test & Evaluation Process Guidelines*, April 2002 (http://fast.faa.gov/test_evaluation/test_eval_toc.html)
- *Open-Source Security Testing Methodology Manual*, April 25, 2001 (http://www.ideahamster.org)
- *National Airspace System (NAS) Subsystem Protection Profile (PP) Template*, version 1.0, March 2002
- FAA *Security Test Plan and Test Results Report Template*, version 2.1, June 22, 2001
- Common Criteria, *Common Methodology for Information Technology Security Evaluation*, CEM-99/045, Part 2: Evaluation Methodology, Version 1.0, August 1999, (http://www.niap.gov)
- FAA *Information Systems Security Program Handbook*, Version 3, February 2002
- FAA *National Airspace System System Engineering Manual*, version 1, http://www.faa.gov/asd/SystemEngineering/index.htm

---

[11] The FAA uses the terms SLS and SRD as the name for the government's statement of requirements or specifications.

- NIST Special Publication 800-26: *Self-Assessment Guide for Information Technology Systems*, August 2001, (http://csrc.nist.gov/publications/nistpubs/index.html)
- NIST Special Publication 800-42 *Guideline on Network Security Testing*, draft February 2002, (http://csrc.nist.gov/publications/nistpubs/index.html)

C.1.2 Acceptance Testing Integration with SCAP Testing

FAA Order 1370.82 *ISS Program* requires all FAA systems to be approved under the FAA Security Certification and Authorization Process (SCAP). An ST&E plan and test report must be included in the SCAP documentation. FAA Order 1370.82 does not provide guidance on the actual security testing.

Security testing as part of acceptance testing for systems developed under contract is not necessarily the same as security testing as part of a SCAP. The reasons for this distinction include:

- Acceptance testing can only address the requirements specific to the contract.
- The Security Plan frequently includes non-technical countermeasures, such as:
  - Physical protection
  - Administrative procedures
  - Operational Procedures
  - Continuity of operations plans
  - Redundancy
- Changes in the environment that may affect Certification and Authorization are not germane to contractual acceptance, such as:
  - Change in law or policy
  - Program change or redirection
  - Change of personnel

The objective of security testing is to assess the implementation of the security architecture and design, including:

- Ascertaining that security features have been implemented as documented.
- Validating the correct implementation of the security features.
- Confirming system conformance with the defined requirements.

ACB-250 (previously ACT-250) has indicated that it would examine the distinction between acceptance testing and SCAP testing as part of the overall test program. ACB-250 stated that their goal was to make Operational Test & Evaluation (OT&E) testing, i.e., contract acceptance testing, and SCAP testing the same. Although acceptance testing by the

developer can only address requirements specific in the contract, OT&E does not have this limitation. By having a complete set of security requirements in time and by having the security mitigation plan completed before starting OT&E, redundancy in these activities can be eliminated. See Section 4 for further discussion of OT&E.

C.1.3 FAST Acquisition Management System Test & Evaluation Process Guidelines

The *FAA Acquisition System Toolset* (FAST) includes the "Acquisition Management System Test & Evaluation Process Guidelines" (FAA, 2001c) at http://fast.faa.gov/test_evaluation/pg2.html. The following extracts from this Toolset express fundamental FAA requirements for security acceptance testing. Citations for safety are included because of the close relationship of safety and security.

FAST 3.2 Solution Implementation and In-Service Management Test and Evaluation

> The most significant test and evaluation (T&E) activities associated with the acquisition and delivery of new FAA Systems are conducted during the Solution Implementation Phase. During this phase, the test strategy is implemented through a series of tests that includes development test (DT), operational test (OT), production acceptance test (PAT), Site Acceptance Tests (SAT), Field Familiarization and, for designated systems, independent operational test and evaluation (IOT&E). Objectives for this series of tests are developed to verify that requirements have been met. The series of tests may verify the same requirement more than once. Guidelines regarding the amount of parallel testing, repeat testing in different test environments, and regression testing necessary to produce a comprehensive, cost-effective test program are program-specific and should be addressed during test strategy and test plan development. …. Development test, system test, and key site test verify that the system is compliant with physical and information security requirements

FAST 3.2.4.1 Solution Implementation Operational Test (OT)

> The primary objective of OT is to demonstrate that a new system is operationally effective and operationally suitable for use in the NAS, and that the NAS infrastructure is ready to accept the system…. The major components of OT are integration tests, performance tests, effectiveness tests, and suitability tests. OT integration testing verifies that the system interfaces with the existing elements of the NAS and that the NAS can operate with the new subsystem at the performance levels required…. OT effectiveness testing evaluates the degree to which a product accomplishes its mission when used by representative personnel in the expected operational environment. This testing includes capacity and NAS loading, degraded mode operations, safety, security, and transition switchover …. OT suitability testing evaluates the degree to which a product intended for field use satisfies its availability, compatibility, interoperability, reliability, maintainability, safety, and human factors. In addition, logistics supportability, documentation, certification criteria, system installation and operating procedures, transition and training requirements are validated.

FAST 3.2.4.2 In-Service Management System Test

> System Test is performed independent of the developer, under conditions that, as close as possible, accurately simulate the operational environment…. Features/performance that cannot be fully verified during this phase of T&E are deferred to the Key Site Test…. It also verifies that the modified system interfaces with the existing elements of the NAS as specified by the Interface Control Document (ICD)…. The ISM operational effectiveness testing evaluates the degree to which the modified system accomplishes its mission. This testing includes capacity and loading, degraded mode operations, safety, security, and system and support system regression.

There are two FAA T&E phases that express fundamental FAA requirements for security acceptance testing. These two phases are Solution Implementation (SI) and In-Service Management System Test (IMST), which are described in the following two extracts from FAST (FAA, 2002c). Citations for safety are included because of the extremely close relationship of safety and security.

C.2 Solution Implementation

The most significant T&E activities associated with the acquisition and delivery of new FAA Systems are conducted during the Solution Implementation (SI) Phase. SI system tests are designed to accomplish two objectives: 1) verify the success of all requirements associated with the acquisition of a system, and 2) verify that the system is ready for operational use. The system tests also answer the questions raised by the Critical Operational Issues (COIs) contained in the Requirement Document (RD).

The SI phase typically begins with refinement and expansion of the Integrated Program Plan (IPP) leading to a full-scale development, Commercial-Off-The-Shelf/Non-Developmental Item (COTS/NDI) procurement or operational prototype. SI system tests (which include DTs, OTs, PATs, and site acceptance tests (SAT), independent operational test and evaluation (IOT&E), and field familiarization) are performed by various FAA organizations to verify that requirements have been met and that the system is ready for operational use. These system tests are described in FAST.

SI System Tests verify that the system is compliant with the physical and information security requirements.

C.3 In-Service Management System Test

System Test is performed independent of the developer, under conditions that, as close as possible, accurately simulate the operational environment. Features/performance that cannot be fully verified during this phase of T&E are deferred to the Key Site Test. System Test also verifies that the modified system interfaces with the existing elements of the NAS as specified by the Interface Control Document (ICD). The ISM operational effectiveness testing evaluates the degree to which the modified system accomplishes its mission. This testing includes capacity and loading, degraded mode operations, safety, security, and system and support system regression.

The In-Service Management phase illustrated in Figure C-1 includes recertification ST&E. Existing, operational systems, sometimes called *legacy systems*, require periodic recertification. Recertification and reauthorization are required by FAA Order 1370.82:

- Every 3 years
- If there is a major system or environmental change that impacts the security posture of the system, including:
  - New or additional connectivity to other information systems
  - Major hardware/software changes
  - Whenever a major security breach has occurred

Some testing of installed operational systems repeats testing of developmental systems while other testing is unique to the operational in-service phase. The FAA ISS Handbook (FAA, 2002b) provides a framework for satisfying the requirements set forth in Federal and FAA policy, such as FAA Order 1370.82. This handbook was written with the goal to provide a consistent process to follow for system certification and authorization, and to offer a means for enhancing information systems security organization-wide by incorporating effective current practices and addressing weaknesses and gaps where necessary. The FAA ISS Handbook defines a 5-phase approach to meet the ISS security requirements. This approach is designed to accommodate the SCAP requirements. In addition, the handbook includes templates for required documents that must be produced for the SCAP.

Appendix D

Security Test and Evaluation Process

D.1 General Security Test and Evaluation Process

A general approach to ISS testing is illustrated in Figure D-1. Each box in Figure D-1 identifies general activities required to accomplish the goals of the Security Test and Evaluation (ST&E), which are to determine how well the system supports the established security requirements and identify any unsupported requirements or requirements that are not fully supported. Both developer testing and independent testing are part of this process.

Figure D-1. General Test & Evaluation Process

More details of each of the general activities shown are described below. This Appendix supplements Appendix C by focusing on Information System Security (ISS). Concepts and procedures from the *Common Evaluation Methodology* (CEM) (CC, 1999) and the National Institute of Standards and Technology (NIST) *Guideline on Network Security Testing*, Special Publication 800-42 (Wack, 2002) , which was available in draft at the time of this report's publication, are employed as examples of best commercial practice. Security testing by the developer is complemented by independent testing. Consequently, many of the activities in Figure D-1 will occur in both developer and Federal Aviation Administration (FAA) domains.

D.2 FAA Strategy

The FAA should require a schedule and outline of deliverables from the developer in support of testing. Agreement on the general form of the test plans and other supporting documentation will be beneficial. The developer products should be available to the FAA on a schedule that supports testing consistent with the master schedule for FAA System. The developer is in the best position to maximize the probability of successful testing.

Provision should be made for full regression testing of developer products. There is a tendency to omit regression testing from the schedule on the excessively optimistic assumption that no flaws will be found and no rework will be required. It is much more realistic to anticipate a need for regression testing and just possibly complete the work ahead of schedule.

One important side effect of FAA analysis and testing is increased understanding on the architecture and design of the FAA System. At the conclusion of testing, the FAA should be in possession of sufficient information to operate and maintain the FAA System.

The FAA must be vigilant to ensure that the scope is reflected in the developer's test plans. There is a natural tendency to focus on the immediate problem of completing the terms of the contract, loosing sight of the broader context. The vulnerability of FAA System and the FAA infrastructure after system integration is critically dependent on the developer's architecture and design.

D.3 Identify Requirements

The security specifications to be tested should be drawn from the appropriate security specifications for the system. Security specifications may be documented in different sources such as System Level Specification (SLS), Protection Profile (PP), Security Plan, Mitigation/Remediation Plan, and Statement of Work (SOW). The identified security specifications for the FAA System will drive the development of the security test plan.

As mentioned in Section 1.3.2, security testing as part of acceptance testing for systems developed under contract, is not necessarily the same as security testing for a Security Certification and Authorization Package (SCAP). The reasons for this distinction include:

- Security testing as part of system acceptance testing can only address the security requirements in the contract.
- Security testing as part of a SCAP can address security requirements in the mitigation plan, security plan, and other requirements documents. A Security Plan can include non-technical countermeasures (e.g., physical protection and administrative procedures).

Although acceptance testing by the contractor can only address requirements specific to the contract, Operational Test and Evaluation (OT&E) does not have this limitation. By having a complete set of security requirements in time and by having the security mitigation plan completed before starting OT&E, OT&E can serve both objectives. The above distinction implies there are two types of security test requirements: Functional Security Test Requirements and Security Remediation/Mitigation Test Requirements.

- **Functional Security Test Requirements**. These security tests requirements are specified in the FAA System *Protection Profile*, Statement of Work (SOW) and/or SLS. These requirements are usually defined as contractual security test requirements. They should be satisfied during acceptance testing. Typically, an ISS functional test plan and results are prepared to satisfy the contractual security test requirements.

- **Remediation/Mitigation Test Requirements**. Per the FAA ISS Handbook, Security testing as part of a SCAP occurs after Remediation/Mitigation. Given this sequence in a SCAP, the security testing should be done against the mitigation items identified in the Mitigation Plan. To show thoroughness of the security testing, the ISS functional test plan and results can be referenced.

Security requirements to be tested should be numbered and clearly identified for tracing and auditing purposes. The security test requirements should be listed in the form of a verification matrix. The security requirements should be included as part of the security test plan. Each security requirement should be mapped in a meaningful way to a test procedure/script. Early involvement by the security engineer in the security test requirement definition and planning is helpful in ensuring the appropriate security requirements are addressed and in understanding of roles and responsibilities.

D.3.1 Security Functional Requirements

The objective of security testing is to validate the security functional requirements of the FAA System. The functional requirements are categorized in the FAA System and included in the SLS as described in Section C.1.1. The SLS specifications have been augmented with two assurance requirements and FAA policy requirement. Below is the list of functional security requirements.

- Identification and Authentication
- Security Audit
- Security Management
- Cryptographic Support
- Network Security Protection
- Application Data Protection
- Protection of Security Data and Mechanisms
- Resource Utilization
- User Session Access Control
- Trusted Path

Two additional security assurance requirements and one FAA policy requirement follow.

- Configuration Management (CM)
- Data Management

- Internet Access

The category of functional requirements from the *NAS System Protection Profile Template* (SPPT) is used to structure the subject areas for the ISS testing guidelines presented later.

D.3.2 Testing NAS PP Security Specifications

The objective of security testing is to demonstrate that the FAA System satisfies the security functional and policy specifications. Testing provides assurance that the FAA System satisfies at least the security functional specifications, although it cannot establish that the FAA System provides security capabilities beyond what was specified. The emphasis is on confirmation that the FAA System operates according to its specification. This will include both positive testing based on functional requirements and negative testing to check that undesirable behavior is absent. The system test requirements identified below are to ensure comprehensive consideration of the ISS testing. These requirements should be addressed by the security test plan and test procedures.

The CC tasks the evaluator to confirm that the information provided meets all requirements for content and presentation of evidence. The following specifications from version 1 of the *SPPT* have been augmented as part of the research leading to this report.

SPPT 6.8.1 Testing Coverage

This specification addresses those aspects of testing that deal with completeness of test coverage. The objective is to establish that the FAA System has been tested against its security functional specification in a systematic manner. It addresses the extent to which the FAA System Security Function is tested, and whether or not the testing is sufficiently extensive to demonstrate whether the FAA System Security Function operates as specified.

Statement of Work Elements

a. The developer shall provide an analysis of the test coverage.

Data Item Description Elements

b. The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the FAA System Security Function as described in the functional specification.

c. The analysis of the test coverage shall demonstrate that the correspondence between the FAA System Security Function as described in the functional specification and the tests identified in the test documentation is complete.

SPPT 6.8.2 Testing Depth

Depth deals with the level of detail to which the developer tests the FAA System. The objective of testing is to counter the risk of missing an error in the development of the FAA System. Testing that exercises specific internal interfaces can provide assurance not only that the FAA System exhibits the desired external security behavior, but also that this behavior stems from correctly operating internal mechanisms. Testing at the level of the system components, in order to demonstrate the presence of any flaws, provides assurance that the FAA System components have been correctly implemented and integrated.

Statement of Work Elements

a. The developer shall provide the analysis of the depth of testing.

Data Item Description Elements

b. The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the FAA System Security Function operates in accordance with its high-level design.

SPPT 6.8.3 Security Functional Tests

Security functional testing performed by the developer establishes whether the FAA System exhibits the security properties necessary to satisfy the security functional specifications.

Statement of Work Elements

a. The developer shall test the FAA System and document the results.

b. The developer shall provide test documentation.

Data Item Description Elements

c. The test documentation shall consist of test plans, test procedure descriptions, expected test results, and actual test results.

d. The test plans shall identify the security functions to be tested, the test tools to be used, and describe the goal of the tests to be performed.

e. The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

f. The expected test results shall show the anticipated outputs from a successful execution of the tests.

g. The test results from the developer execution of the tests shall demonstrate whether each tested security function behaved as specified.

h. The test documentation shall include an analysis of the test procedure ordering dependencies.

SPPT 6.8.4 Preparation for Independent Testing

Independent testing demonstrates whether the security functions perform as specified and helps counter the risk of an incorrect assessment of the test outcomes on the part of the developer that results in the incorrect implementation of the specifications, or overlooks code that is non-compliant with the specifications.

Statement of Work Elements

a. The developer shall provide the FAA System for testing.

Data Item Description Elements

b. The FAA System shall be suitable for testing.

Additional Evaluator Action Elements

c. The evaluator shall test a subset of the trusted security function as appropriate to confirm that the FAA System operates as specified.

D.4 Develop Test Plan

The purpose of the Security Test Plan is to provide a plan for ST&E. ST&E is a means of verifying that the security features intended to implement the FAA System security policy have been implemented correctly. The test plan should be driven by the identified security specifications for the system. Various methodologies may be used to test the system's adequacy in determining whether security specifications are met. The security test plan and security test results may take several forms depending on whether the system is a prototype, in development, currently operating or undergoing modifications. An example of a security test plan outline is provided in Appendix E.

D.5 Determine Types of Tests

Testing of the ISS features can encompass a broad range of tests from a series of formal tests, as a part of the AMS system development and testing process, to a penetration test. This is dependent on whether the system is a prototype, in development, currently operating or undergoing modifications. Therefore, the types of tests required must be tailored to each system test program. Table D-1 contains the types of tests that may need to be planned and a definition for each test type. The list is not all-inclusive.

Table D-1. Types of Tests

Test	Description
Developmental Tests (DTs)	A series of tests designed to verify that system technical and performance requirements specified in the contract and system specification have been met. Performed by the developer and witnessed by William J. Hughes Technical Center (WJHTC) personnel.
Field Familiarization	The purpose is to verify that the site is ready to transition to the new system. Conducted by AT and AF field personnel at each new site after the system has successfully completed installation and checkout.
Operational Tests (OTs)	A series of tests designed to demonstrate the system is operationally effective and operationally suitable for use in the NAS, and that the NAS infrastructure is ready to accept the system. These tests focus on demonstrating operational requirements have been met and that all critical operational issues (COIs) have been resolved, including changes to the security environment. These tests must include both integrity validation and resource consumption testing. For example, tests should included verification of resource management and archiving of audit trail data and system log data. Major components of OT&E are integration tests, suitability tests, and effectiveness tests. The FAA at the WJHTC, an internal or third party, or a field site using field personnel conducts operational testing.
Penetration Tests (PTs) and Vulnerability Assessment (VA)	The evaluator attempts to circumvent the security features of a system to gain access. NOTE: Penetration testing on FAA information systems must have advanced coordination and formal authorization with the DAA for the line of business or staff office that owns the system, the information owner (if not the same as the system owner), and the Office of Chief Counsel. If the penetration test could impact one or more systems for which other DAA's are responsible, then coordination must include all affected DAA's. In addition, all personnel participating in the testing should meet background investigation personnel requirements. See section D.9.3.
Production Acceptance Tests (PATs)	A subset of the design qualification tests conducted on the first article plus quality control testing. The vendor for each system conducts this test before it leaves the factory.
System Tests	A series of tests designed to verify that a FAA System meets its specified requirements. Subsets of system test are development tests, operational tests, production tests and site acceptance tests. Each must verify satisfaction of all requirements associated with a system.

Test	Description
Vulnerability Tests	The evaluator uses commercial and public domain testing tools to attempt to identify security vulnerabilities and modes of compromise that existing security safeguards do not address.
Regression Tests	A series of tests designed to verify the security safeguards introduced in the remediation phase have not altered the required functionality or performance of a system.
Positive Tests	A series of tests designed to verify that a system meets its specified security requirements. Testing of boundary or limit values are included.
Negative Tests	A series of tests designed to verify that a system does not do anything that is contrary to its security specifications. Tests include violation of assumptions and specifications. Testing should also ensure that what it does will not have an adverse effect on any other FAA System.

ST&E, as part of the SCAP, should be performed after remediation/mitigation process and should involve ST&E against the mitigation items. The Penetration Test Plan and result may be required to satisfy the SCAP requirement.

For each security requirement to be tested, a test method should be clearly defined. Table D-2 identifies the categories of test methods to be considered for this effort. Test methods should support testing in a way to provide repeatable and reproducible results. Tests should be designed so that outcomes are self-evident, requiring a minimum of subjective interpretation and administrative resolution. For the developer tests provided, the FAA determines whether the tests are repeatable, and the extent to which the developer's tests can be used for the FAA's independent testing effort. Any security function for which the developer's test results indicate that it may not perform as specified should be tested independently by the evaluator so that an acceptance determination can be made. The FAA determines that functional requirements are stated in such a way that they are testable. The FAA also determines that assurance requirements avoid the need for subjective judgment. Test tools that perform repeatable testing and minimal human interaction/interpretation are necessary. For demonstration, inspection, and test, both automated test tools as well as manual scripted tests and/or checklists may be conducted.

Table D-2. Definition of Test Methods

Methods	Definition	Implementation
A – Analysis	The evaluation using recognized analytical techniques, such as comparing design with requirements.	Accomplished by review of architectural documents.
D – Demonstration	The evaluation by operation, movement, or adjustment under a specific condition to determine the capability to satisfy a stated requirement.	Consist of test scripts that exercise system capabilities, which include Analysis.
I – Inspection	The physical examination or review of the security feature, such as review of a configuration file, software version number/patch level, or procedures.	Consist of checklists for review of system parameters, review of the operational environment, procedures, or personnel interviews, which includes Analysis.
T – Test	The collection, analysis, and evaluation through systematic hands-on measurement under appropriate conditions.	Consists of test scripts that exercise system capabilities.

D.6 Develop Test Procedures

The test procedures should serve as the instructions for the individual who conducts the actual security test. Since these tests will be used to verify whether or not the system is in compliance with the stated security measures, sufficient time should be spent ensuring that each test adequately examines all facets of the corresponding security requirement without ambiguous results. Test procedures should be traced back to the security specifications being tested. Security specifications being tested should be explicitly identified in the test procedures. Test procedures should be explicitly written so they are repeatable. It is possible some specifications are addressed by more than one test procedure, or more often, one procedure may test several specifications.

Test objectivity and completeness is enhanced when the tests are developed by people who were not involved in development. The test team and development teams should be disjoint.

For each test procedure, there should be an explicitly expected result that would verify that the system is in compliance with the stated security specification. If the outcome of the

test procedure does not match the expected result, then the system fails the test and is deemed not to be in compliance with the specific security specification.

Before actual testing, it is important to identify the resources required to execute the test procedures to ensure that they are all available so that the testing can be conducted in a timely manner. If any test procedures require resources that cannot be obtained or are simply not feasible to obtain, then that test procedure should be revised so that can be completed with the available resources. An example of a security test procedure template is shown in Appendix E.

D.7 Perform Tests

Once the security test plan and procedures has been developed, an internal or third party testing team can follow its detailed instructions to perform the security test. This section addresses ISS testing performed by the developer and FAA, and ISS testing on the system test bed and operating system.

D.7.1 Developer Testing

Security functional testing performed by the developer establishes that the FAA System exhibits the security properties necessary to satisfy the security functional specifications. Typically, the developer performs testing to produce documentation describing the system security properties and how the system was produced. The scope of this testing includes the hardware and software and the documentation describing the design, implementation, and security testing.

The developer tests the FAA System and documents the results. The test documentation consists of test plans, test procedure descriptions, expected test results and actual test results. The test plans identify the security functions to be tested and describe the goal of the tests to be performed. The test procedure descriptions identify the tests to be performed and describe the scenarios for testing each security function. These scenarios include any ordering dependencies on the results of other tests. The expected test results show the anticipated outputs from a successful execution of the tests. The test results from the developer execution of the tests demonstrate that each tested security function behaved as specified.

Random sampling of developer tests is intended to provide confirmation that the developer has carried out his planned test program, and has correctly recorded the results. The detail and quality of the developer's functional test results will influence the size of sample selected. It is recognized that repetition of all developer tests may be feasible and desirable in some cases, but may be very arduous and less productive in others.

It is advisable that the developer's ISS testing requirements be clearly specified. For a system under contract, such as FAA System, the developer's ISS testing requirements are in the SOW.

D.7.2 FAA Independent Testing and Evaluation

FAA independent functional security testing may take the form of repeating the developer's functional tests, in whole or in part. It may also take the form of the augmentation of the developer's functional tests, either to extend the scope or the depth of the developer's tests, or to test for published public domain security weaknesses that could be applicable. Published security weaknesses are often accompanied with "patches" and other remediation, the presence of which may be tested; this is referred to as "version testing."

The developer should provide an equivalent set of resources to those that were used in the developer's functional testing. The intent is that the developer should provide the FAA evaluator with materials necessary for the efficient reproduction of developer tests. This may include such things as machine-readable test documentation, and test programs. The FAA evaluator tests a subset of the security functions as appropriate to confirm that the security functions operate as specified. The FAA evaluator executes a sample of tests in the test documentation to verify the developer's test results.

Developer testing and FAA independent testing are complementary, and an appropriate mix must be planned, which takes into account the availability and coverage of test results, and the functional complexity of the system. A test plan should be developed that is consistent with the level of other assurance activities, and which, as greater assurance is required, includes larger samples of repeated tests, and more independent positive and negative functional tests. Positive testing is based on functional requirements, while negative testing checks that undesirable behavior is absent.

FAA independent testing includes the COTS and FAA-furnished components. Some of these components, such as operating systems and communications protocol drivers, are highly integrated in the developer's product. Their testing will be an integral part of testing the developer's product. Other components, such as a communications network, will be external to the developer's product. The developer's product will connect to and interoperate with such components. These components will be addressed as part of integration testing.

D.7.3 Developer Test Actions and Specifications

The developer test specifications in the PP are found in Section D.3.2 above: SPPT 6.8.1 Testing Coverage, SPPT 6.8.2 Testing Depth, SPPT 6.8.3 Security Functional Tests, and SPPT 6.8.4 Preparation for Independent Testing.

D.7.4 Independent Test Actions and Specifications

The following specifications from the CC were not included in the SPPT because of the way that document was anticipated to be used in acquisition and contracting. These specifications add specificity to the FAST "Acquisition Management System Test &

Evaluation Process Guidelines" (FAA, 2001c). The underlined reference associated with each specification (e.g., AVA_VLA.2.3E) refers to the CC distinguished identifier composed of class, family, and component.

Independent Vulnerability Analysis complements the Developer Vulnerability Analysis. Vulnerability Analysis defines requirements directed at the identification of exploitable vulnerabilities introduced in the architecture and design, construction, operation, misuse, or incorrect configuration of the FAA System. Independent vulnerability analysis is often part of independent verification and validation. The distributed nature of the NAS Subsystem necessitates extending the scope to include both stand-alone and network-based vulnerabilities. The parenthetical references to the CC enable the interested reader to easily obtain additional information.

D.7.4.1 Independent Vulnerability Analysis (AVA_VLA)

Independent vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the analysis of the architecture, design, construction and operation of the FAA System or by other methods (e.g., by flaw hypotheses), could allow users to violate the FAA System Security Policy or reduce the security of any other part of the NAS.

Statement of Work Elements

a. The evaluator shall perform and document an independent vulnerability analysis of the FAA System implementation, the Descriptive High-Level Security Design, the Descriptive High-Level Functional Design, and the NAS policies and procedures searching for ways in which a user can violate the Security Policy of this or any other FAA System. (AVA_VLA.2.3E)

b. The analysis shall incorporate the statement of the FAA System security environment developed specified in the FAA System Security Environment (ASE_ENV), including the threats originating in systems external to the FAA security domain.

Data Item Description Elements

c. The evidence shall show that FAA System has been examined for published and other well-known and obvious vulnerabilities and flaws. (AVA_VLA.2.2C)

d. The evidence shall show that the search for vulnerabilities is systematic. (AVA_VLA.3.3C)

D.7.4.2 Misuse Documentation (AVA_MSU)

These requirements investigate whether the FAA System can be configured or used in a manner that is insecure but that an administrator or user of the FAA System would reasonably believe to be secure. The objective is to ensure that misleading, unreasonable and

conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed.

Statement of Work Elements

a. The developer shall provide guidance documentation. (AVA_MSU.2.1D)

b. The developer shall document an analysis of the guidance documentation. (AVA_MSU.2.2D)

Data Item Description Elements

c. The guidance documentation shall identify all possible modes of operation of the FAA System (including operation following failure or operational error), their consequences and implications for maintaining secure operation. (AVA_MSU.2.1C)

d. The guidance documentation shall be complete, clear, consistent and reasonable. (AVA_MSU.2.2C)

e. The guidance documentation shall list all assumptions about the intended environment. (AVA_MSU.2.3C)

f. The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls). (AVA_MSU.2.4C)

g. The analysis documentation shall demonstrate that the guidance documentation is complete. (AVA_MSU.2.5C)

D.7.5 Test Environment

It is intended that the complete testing philosophy (i.e., automated tools, checklists, documentation review) should be applied to the particular FAA System test bed to determine the security posture. Tests performed on the system test bed should be designed to determine whether the system is susceptible to various forms of attack or misconfiguration. This includes technical vulnerability tests that consist of broad "vulnerability scans" performed by automated tools designed to rapidly identify known vulnerabilities on hosts and network devices comprising the system. The test team should also conduct scripted tests or checklists of security features and mechanisms designed to demonstrate compliance with requirements and/or proper configuration of security features. Together, this suite of tests provides a comprehensive body of evidence of the system's resistance to attack. Testing should be generally guided using these resources but may be modified as necessary to provide the most complete picture of the systems reviewed. Tests should be conducted in close coordination with individuals familiar with administration of the system, yet independent of the development effort, to draw on their expertise of system operation.

D.8 Record Test Results

Security test results should be recorded in a Security Test Report. Any deviations from the planned tests should be documented. Information (e.g., IP addresses) that can be used to compromise the security of the system, should be precluded for the Security Test Report. Appendix F contains a template for a security test report.

D.9 Operational System Testing

Some testing of installed operational systems repeats testing of developmental systems while other testing is unique to the operational in-service phase. The NIST *Guideline on Network Security Testing* describes a methodology for using network based tools for testing systems for vulnerabilities. The primary aim of the NIST Guideline is to help administrators and managers get started with a program for testing on a routine basis. The methodology recommends focusing first on those systems that are accessible externally (e.g., firewalls, web servers) and then moving on to other systems as resources permit. The NIST Guideline includes many pointers to various testing applications and contains more detailed descriptions of several of the more popular test tools. The reader is cautioned that attacks, countermeasures, and test tools tend to change rapidly and often dramatically. Current information should always be sought. Testing will change along with changes in technology, threats, and needs.

The security testing should include manual and automated review of a sampling of critical files from the live system components and review of procedures. The requirements that are addressed on the operational system should be annotated in a Security Requirements Verification Matrix (SRVM). This test approach has been designed to avoid any possible disruption to ongoing activities. Operational systems should NOT be subjected to any tests intended to demonstrate or exploit these vulnerabilities. Tests should be conducted in close coordination with individuals familiar with administration of the system to draw on their expertise of system operation and identify any potential for system disruption.

Operational system security testing should be integrated into an organization's security program as a normal part of the duties of security administrators to evaluate system security mechanisms and validate that systems are operating according to the FAA System security policies and system security requirements. Organizations should prioritize operational system testing activities according to system criticality, testing costs, and the benefits that testing will provide.

Security gaps can open up as a result of system changes and/or advances in hacker technology. Testing on an on-going basis is the only way to know if new security gaps are opening up. Hackers don't try to penetrate systems just once, so testing shouldn't take place just once a year. Some security vulnerabilities are more likely to show up when network traffic is heavy (i.e., fragmented packet security gaps) and some are more likely to show up when network traffic is light (i.e., predictable TCP or IP sequences). Tests should be

conducted at different times: weekdays, weekends, days, nights, holidays, and non-holidays. Test composition should also vary from one occasion to the next.

Routine testing of operational system can greatly reduce the chances of compromise by helping to ensure that critical systems (e.g., firewalls, routers, servers) are configured, maintained, and operated according to the applicable security policy. Exploitation of a system could have a costly impact on the NAS operations. Operational system testing can be a valuable and cost effective measure of protecting a network and preventing costly compromise.

The purpose of the NIST Guideline is to provide guidance on when and how to perform tests for security vulnerabilities and policy implementation. The NIST Guideline identifies network testing requirements and how to prioritize testing activities with limited resources. It describes security testing techniques and tools, avoiding redundancy and duplication of effort by providing a consistent approach to network security testing throughout an organization, and provides a feasible approach for varying levels of network security testing as mandated by an organization's mission and security objectives.

The primary reason for testing a system is to identify potential vulnerabilities and subsequently repair them. Testing is a fundamental security activity that can be conducted to achieve a secure operating environment while fulfilling an organization's security requirements. Testing allows an organization to accurately assess their system's security posture. Also, testing, using the techniques recommended in the NIST Guideline, allows an organization to view its network the same way an attacker would, thus providing additional insight and advantage.

Security testing provides insight into other system life cycle activities. Security testing results should be documented and made available for staff involved in other IT and security related areas. Specifically, security testing results can be used in the following ways:

- As a reference point for corrective action.
- Defining mitigation activities to address identified vulnerabilities.
- As a benchmark for tracing an organization's progress.
- To assess the implementation status of system security requirements.
- To conduct cost/benefit analysis.
- To enhance other lifecycle activities, such as risk assessments, C&A, and performance improvement efforts.
- To measure changes over time and the extent to which such change was anticipated.

There are several different types of security testing, described below and summarized in Tables D-3 and D-4. The following types of testing are described:

- Network Mapping
- Vulnerability Scanning
- Penetration Testing
- Security Test & Evaluation
- Password Cracking
- Log Review
- Integrity and Configuration Checkers
- Malicious Detection
- Modem Security

Often, several of these testing techniques are used in conjunction to gain more comprehensive assessment of the overall network security posture. For example penetration testing almost always includes network mapping and vulnerability scanning to identify vulnerable hosts and services that may be targeted for later penetration. None of these tests by themselves will provide a complete picture of the network or its security posture.

A concise monthly testing report should be prepared suitable for both senior FAA management and hands-on technologists. The report should contain:

- An executive summary explaining how the testing was performed, what was tested, how many tests were conducted, and the number of security gaps that were identified.
- An assessment of the FAA's risks. A risk rating should be provided for each of the major types of potential vulnerabilities.
- An explanation of each of the FAA's system security vulnerabilities. Note that this information will probably be considered security-sensitive and must be marked and protected accordingly.
- Each explanation should include both the business risk as well as the technical details. The technical details should be very specific as to which machines, ports, and services, have which security gaps, and how each could be exploited. However, in order to maintain testing objectivity the explanations should not include recommendations or consulting advice.
- A list of the agency's hosts that are visible to outsiders. This list should include all the machines that are visible, not just those that contain security gaps.
- An appendix defining the vulnerabilities tested. This will provide a framework for reviewing the risk assessment and the explanation of each security gap.

D.9.1 Network Mapping

Network mapping involves using a port scanner to identify all active hosts connected to an organization's network, network services operating on those hosts (e.g., file transfer protocol [FTP] and hypertext transfer protocol [HTTP]), and the specific application running the identified service. The result of the scan is a comprehensive list of all active hosts and services operating in the address space scanned by the port scanning tool. The name "network map" is a misnomer, as the port scanner sees the network as flat address space and does not typically provide any meaningful graphical representation of the scanned network.

All basic port scanners will identify active hosts and open ports, but some scanners provide additional information on the scanned hosts. In addition, some scanners will assist in identifying the application running on a particular port. A major limitation of using port scanners is that while they identify active hosts, services, applications and operating systems, they do not identify vulnerabilities except for common vulnerabilities that may be inferred. Organizations should conduct network mapping to:

- Check for unauthorized hosts connected to the organization's network.
- Identify vulnerable services.
- Identify deviations from the allowed services defined in the organization's security policy.
- Prepare for penetration testing.
- Network mapping results should be documented and identified deficiencies corrected.

The following corrective actions may be necessary as a result of network mapping:

- Disconnect unauthorized hosts.
- Disable or remove unnecessary and vulnerable services.
- Modify vulnerable hosts to restrict access to vulnerable services to limited number of required hosts (e.g., host level firewall or TCP wrappers).
- Modify enterprise firewalls to restrict outside access to known vulnerable services.

D.9.2 Vulnerability Scanning

Vulnerability scanners are commonly used in many organizations. Vulnerability scanners take the concept of a port scanner to the next level. The vulnerability scanner identifies not just hosts and open ports but any associated vulnerabilities automatically instead of relying on human interpretation of the results. Most vulnerability scanners also attempt to provide information on mitigating discovered vulnerabilities. Vulnerability

scanning can be considered part of a continuum, where the next capability is vulnerability assessment, described in the following Section D.9.3.

Vulnerability scanners are, essentially, software that checks the relative health of computers and other devices by probing for a finite number of problems that could leave them open to attack. Some examples include:

- Buffer overflows, in which sending too much input to a program causes it to fail, allowing the attacker to execute rogue commands on the host system.
- Back doors left in programs by vendors; these are meant to ease support, but if exposed, can give an attacker entry into a system.
- Bugs that can be exploited to force a program to perform an unauthorized operation.

Vulnerability scanners provide system and network administrators with proactive tools that can be used to identify vulnerabilities before an adversary. Vulnerability scanners can help identify out-of-date software versions, vulnerabilities, applicable patches or system upgrades, and validate compliance with, or deviations from, the organization's security policy. For each discovered vulnerability, the scanner will often provide significant information and guidance on mitigating discovered vulnerabilities. In addition vulnerability scanners can automatically make corrections and fix certain discovered vulnerabilities.

Vulnerability scanners can be of two types: network scanners and host scanners. Network scanners are used primarily for mapping an organization’s network and identifying open ports. Host scanners have to be installed on each host to be tested and are used primarily to identify specific host operating system and application misconfiguration and vulnerabilities.

Vulnerability scanners generally only identify surface vulnerabilities and are unable to address the overall risk level of a scanned network. Since vulnerability scanners require more information than port scanners to reliably identify the vulnerabilities on a host, vulnerability scanners tend to generate significantly more network traffic than port scanners. Vulnerability scanners rely on constant updating of the vulnerability database in order to recognize the latest vulnerabilities. Vulnerability scanners are better at detecting well known vulnerabilities at the expense of more esoteric ones, primarily because it is impossible for any one product to incorporate all known vulnerabilities in a timely manner. Vulnerability scanning may adversely impact system performance, up to and including causing a system crash. Vulnerability scanners provide the following capabilities:

- Identifying active network nodes.
- Identifying active and vulnerable services (ports) on hosts.
- Identifying application and banner grabbing.

- Identifying operating systems.
- Identify misconfiguration of system resources and services.
- Identifying vulnerabilities associated with discovered operating systems and applications.
- Testing compliance with host application usage/security policies.
- Establishing a foundation for penetration testing.

Vulnerability scanning results should be documented and discovered deficiencies corrected. The following corrective actions may be necessary as a result of vulnerability scanning:

- Upgrade or patch vulnerable systems to mitigate identified vulnerabilities as appropriate.
- Deploy mitigating measures (technical or procedural) if the system cannot be immediately patched (e.g., application system upgrade will make the application running on top of the operating system inoperable), in order to minimize the probability of this system being compromised.
- Tighten configuration management program and procedures to ensure that systems are upgraded routinely.
- Assign a staff member to monitor vulnerability alerts and mailing lists, examine their applicability to the organization's environment and initiate appropriate system changes.
- Modify the organization's security policies, architecture, or other documentation to ensure that security practices include timely system updates and upgrades.

Some older equipment, or process or memory constrained equipment, does not tolerate current vulnerability scanning tools well. The tools can cause the older machines to freeze. In cases where there are multiple interconnected machines/processes this can cause a cascading effect. Tests that would normally be considered non-destructive can have a ripple effect with some older equipment.

D.9.3 Penetration Testing

Penetration testing (pen test or PT) has been described as the gold standard and acid test for information system security. This section provides guidance regarding penetration testing focused on issues that pertain to systems that are involved with real-time operations considered mission critical, such as the NAS. Issues and recommendations concerning PT were first addressed in Section 3.4. Evaluation actions for devising and conduction PT are found in Section B.8.3.

D.9.3.1 Definition, Purpose, and Variations of Penetration Testing

PT is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation. The purpose of penetration testing is to identify vulnerabilities with a system architecture, not previously identified, by which an adversary could gain unauthorized access by using common and/or unique tools and techniques. It is assumed that once identified, the vulnerabilities can be repaired, redesigned, or otherwise protected. The evaluator is not necessarily the best person to close the vulnerability. Separation of duties also argues for different people performing the roles.

Vulnerability assessment (VA) is a variant of PT. VA is the collection and analysis of system and network architecture, system configuration, and application design/code in order to identify as many as possible exploitable vulnerabilities. VA can be considered an extension of Vulnerability Scanning with less automation and more analysis. In contrast, a PT may focus on a smaller number of vulnerabilities and may terminate after demonstrating that vulnerabilities exist. VA emphasizes analysis while PT emphasizes experimental testing.

Based on these definitions, a PT is far more likely to cause disruption of service than a VA. The side effects of a VA should be limited to performance degradation. However, there is no guarantee that a system crash/failure will not occur as a result of a VA.

There are three degrees of freedom available for penetration testing: (1) unsupervised, such as case where the evaluator is alone at a terminal, (2) partially supervised, such as the case where the evaluator is accompanied by a qualified system administrator, and (3) supervised, such as the case where the evaluator is under the direct control of a qualified system administrator. In the case of supervised penetration testing, the evaluator pauses after each action at the terminal and receives a go/no-go decision from a qualified system administrator. The degree of supervised penetration testing progress is controlled by the system administrator.

Penetration testing can be overt or covert. These two types of penetration testing are commonly referred to as Blue Teaming and Red Teaming. Blue Teaming involves performing a penetration test with the knowledge and consent of the organization's IT staff. Red Teaming involves performing a penetration test without the knowledge of the organization's IT staff but with full knowledge and permission of the responsible management. Some organizations designate a trusted third party for the Red Teaming exercises to ensure that an organization does not take measures associated with the real attack without verifying that an attack is indeed under way (i.e., the activity they are seeing does not originate from an exercise). The trusted third party provides an agent for the testers, the management, and the IT and security staff that mediates the activities and facilitates communications.

Of the two types of penetration tests, Blue Teaming tends to be the least expensive and most used. Red Teaming, because of its stealth requirements, requires more time and expense. A penetration test can be designed to simulate an inside and/or an outside attack. Where vulnerability scanners only check that a vulnerability may exist, the attack phase of a penetration test exploits vulnerability, only within identified parameters and consistent with the test plan, confirming its existence.

Penetration testing can be an invaluable technique to any organization's information security program. This may be the only way to determine operational and configuration deficiencies. However, it is a very labor intensive activity and requires great expertise to minimize the risk to targeted systems. It may slow the organization's networks response time due to network mapping and vulnerability scanning.

D.9.3.2 Recommended Penetration Testing Strategy

The use of PT in an operational, or production, command and control system, like the NAS, requires additional care and consideration. Utilization of penetration testing should be avoided if at all possible and only after less intrusive means have been exhausted. PT of the live production system may be the only way to discover configuration problems that involve multiple systems or that include the human-computer interface.

One alternative is to make a “snap shot” or image copy of the system(s) to be tested, including all configuration parameters and installations customization and duplicate that system using the image copy on a test configuration at the Technical Center. The remainder of the NAS would be simulated or otherwise represented by the Technical Center test configuration. Penetration testing would be conducted on the image copy. In general, vulnerability scanning, VA, and PT should be conducted at the Technical Center before there is any testing of the operational NAS. Convincing evidence of risk should be required before testing on the operational NAS would be authorized.

MITRE recommends that the FAA establish a policy for penetration testing in FAA Systems that balances the risks and benefits and provides uniform procedures and identified the level of management authorization required.

When an organization tests the results of their own advice, products, or services, they always look good. Penetration testing should be performed by a third party that is immune from any conflicts of interest.

D.9.3.3 Rules of Engagement

Since penetration testing is designed to simulate an attack and use tools and techniques that may be restricted by law, federal regulations, and organizational policy, it is imperative to obtain written permission for conducting penetration testing prior to starting. This written

permission, often called the rules of engagement, and captured in the penetration test plan, should include:

- Specific systems to be tested, including network addresses/ranges to be tested.
- The scope of testing (e.g., interfaces with other systems and how far into these systems testing will go).
- Any restricted hosts (i.e., hosts, systems, subnets, not to be tested).
- A list of acceptable testing techniques (e.g., social engineering, DoS) and tools (e.g., password crackers, network snifters).
- The extent of testing (e.g., which level, or impact, of vulnerabilities will be exploited).
- Times that scanning is to be conducted (e.g., during business hours, after business hours).
- IP addresses of the machines from which penetration testing will be conducted so that administrators can differentiate the legitimate penetration testing attacks from actual hacker attacks.
- Points of contact for both the penetration testing team and the targeted systems and networks.
- Assurance that notice has been given to test conduits and consent has been obtained from test targets.
- Measures to prevent law enforcement being called with false alarms.
- Handling of information collected by penetration testing team.

For example, one organization tests on an operational highly sensitive network. The security testers/assessors are given a range or ranges of IP addresses so that they do not even ping devices outside the test. Exploitation is forbidden since the results of the exploitation could be unpredictable and cause network disruption, but the value of identification of the vulnerabilities which are found is well worth the investment. The system operators are not told about the assessment, so if they observe anomalous activity that could be an attacker, their reaction is reported and captured as part of the test. A trusted agent is employed so that erroneous incident reports are not filed through official channels. Two types of assessments are always performed: a view from the "inside"–that of an authorized user of the system under assessment, and a view from "outside"–that of a user who may have access to the network or media over which the system is operating, but who is not an authorized user of the system.

D.9.4 Security Test and Evaluation

Security Test and Evaluation is an examination or analysis of the protective measures that are placed on an information system once it is fully integrated and operational. The objectives of the ST&E are to:

- Uncover design, implementation, and operations flaws that could allow the violation of security policy.
- Determine the adequacy of security mechanisms, assurances, and other properties to enforce the security policy.
- Assess the degree of consistency between the system documentation and its implementation.

D.9.5 Password Cracking

Password cracking programs can be used to identify weak passwords. Password cracking verifies that users are employing sufficiently strong passwords. Password crackers should be run on the system on a monthly basis or even continuously to ensure correct password composition throughout an organization. Password cracking should be conducted on a dedicated system with very restricted access. The following actions can be taken if an unacceptable number of passwords can be cracked:

- If the cracked passwords were selected according to policy, the policy should be modified to reduce the percentage of crackable passwords. If such policy modification would lead to users writing down their passwords because they are difficult to memorize, an organization should consider replacing password authentication with another form of authentication.
- If cracked passwords were not selected according to policy, the users should be educated on possible impacts of weak password selections. If such violations by the same users are persistent, the management may consider a disciplinary action against those users. Many server platforms also allow the system administrator to set minimum password length and complexity.

D.9.6 Log Reviews

Various system logs can be used to identify deviations from the organization's security policy, including firewall logs, IDS logs, server logs, and any other logs that are collecting audit data on system and network. While not traditionally considered a testing activity, log review and analysis can provide a dynamic picture of ongoing system activities that can be compared with the intent and content of the security policy. Essentially, audit logs can be used to validate that the system is operating according to policies. Log reviews should be conducted at least weekly by a knowledgeable reviewer, regardless of how the results are

used. For the specific purpose of testing implementation of required security configurations, a monthly frequency may be sufficient with the exception of on demand reviews resulting from major system upgrades that require validation. The following actions can be taken if a system is not configured according to policies:

- Reconfigure the system as required to reduce the chance of compromise.
- Change system policy to limit access to the vulnerable system or service.
- Change system policy to limit accesses from the IP subnet that is the source of compromise.

D.9.7 File Integrity Checkers

A file integrity checker computes and stores a checksum for every guarded file and establishes a database of file checksums. It provides a tool for the system administrator to recognize changes to files, particularly unauthorized changes. Stored checksums should be recomputed regularly to test the current value against the stored value to identify any file modifications. A file integrity checker capability is usually included with any commercial host based intrusion detection system.

While an integrity checker is a useful tool that does not require a high degree of human interaction, it needs to be used carefully to ensure that it is effective. A file integrity checker requires a system that is known as secure to create the first reference database. Integrity checkers should be run daily on a selection of system files that would be affected by a compromise. Integrity checkers should also be used when a compromise is suspected for determining the extent of possible damage.

File integrity checkers must be configured properly to recognize files that change frequently during normal operation. The level of effort for configuration may be substantial.

D.9.8 Malicious Code Detectors

Malicious code is generally detected by so-called antivirus software even though the code is not strictly speaking a virus. Other categories of malicious code include worms, Trojans, and malicious mobile code. There are two primary types of antivirus programs available: those that are installed on the network infrastructure and those that are installed on end user machines. Each has advantages and disadvantages, but both used in conjunction are generally required for the highest level of security. A virus detection program cannot offer its full protection unless is has an up-to-date malicious code identification database (sometimes called signatures) that allow it to recognize all malicious code.

D.9.9 Modem Security

In a well-configured network, one of the vulnerable areas often overlooked is the presence of unauthorized modems. A naïve employee may activate an unauthorized modem on his desktop PC, install a remote-control program such as pcAnywhere (without a password), and turn on the modem before going home at night. Maybe the employee wants to dial in after hours and retrieve files off his hard drive. Or, maybe he wants to use the corporate network to surf the Internet free. Vendors providing a modem so that equipment can "call home" or be remotely managed are another common problem; some hardware includes fully integrated modems. These unauthorized modems provide a means to bypass most or all of the security measures in place to stop unauthorized users from accessing a network.

Using telephone scanners called "war dialers," an adversary can dial a list of telephone numbers, in increasing or random order, searching for the familiar modem carrier tone. Once the dialer generates a list of discovered modems, the adversary can dial those numbers to find an unprotected login or easily cracked password to a remote-control program. Just as an adversary can use a war dialer to scan for unregistered modems, security professionals can use similar tools to scan their own networks. Highly distributed systems may make defense war dialing security testing prohibitively difficult. Coordinated auditing with the telephone service organization may be the best possible testing. If defensive war dialing possible, it should be conducted at least annually and performed after hours to limit potential disruption to employees and the organization's phone system. If any unauthorized modems are identified, they should be investigated and removed, if appropriate.

D.9.10 Comparison of the Testing Techniques

Tables D-3 and D-4 provide a comparison of the testing techniques. These tables are extracted from the NIST Guideline and contain characteristics not discussed in this extract.

Table D-3. Comparison of Testing Procedures

Type of Test	Strengths	Weaknesses
Network Mapping	• Fast • Efficiently scans a large number of hosts (approximately 30 seconds per host) • Many excellent freeware tools available • Highly automated (for scanning component) • Low cost	• Does not directly identify known vulnerabilities • Generally used as a prelude to penetration testing not as final test • Requires significant expertise to interpret results • Requires coordination with defensive services group

Type of Test	Strengths	Weaknesses
Vulnera-bility Scanning	• Fairly fast • Efficiently scans a large number of hosts (approximately 2 minutes per host) • Some freeware tools available • Highly automated (for scanning) • Identifies known vulnerabilities • Often provides advice on mitigating discovered vulnerabilities • High cost (commercial scanners) to low (freeware scanners) • Easy to run on a regular basis	• High false positive rate • Generates large amount of network traffic • Not stealthy (e.g., easily detected by IDS, firewall and even end users) • Can be dangerous in the hands of a novice (particularly DoS attacks) • Often misses latest vulnerabilities • Identifies only surface vulnerabilities • Requires coordination with defensive services group
Penetra-tion Testing	• Tests network using the methodologies and tools that hackers employ • Verifies vulnerabilities • Goes beyond surface vulnerabilities and demonstrates how these vulnerabilities can be exploited iteratively to gain greater access • Demonstrates that vulnerabilities are not purely theoretical • Can provide the realism and evidence needed to address security issues • Social engineering allows for testing of procedures and the human element network security	• Requires great expertise • Very labor intensive • Slow, target hosts may take hours/days to .crack. • Due to time required not all hosts on medium or large sized networks will be tested individually • Dangerous when conducted by inexperienced testers • Certain tools and techniques may be banned or controlled by agency regulations (e.g., network snifters, password crackers) • Expensive • Can be organizationally disruptive • Legal complications (get written permission to conduct and make sure all necessary personnel are notified)
Security Testing and Evaluation	• Not as invasive or risky as some other tests • Includes policy and procedures • Generally requires less expertise than vulnerability scanning or penetration testing • Addresses physical security	• Does not verify vulnerabilities • Generally does not identify newly discovery vulnerabilities • Labor intensive • Expensive

Type of Test	Strengths	Weaknesses
Password Cracking	• Quickly identifies weak passwords • Provides clear demonstration of password strength or weakness • Easily implemented • Low cost	• Potential for abuse • Certain organizations restrict use • Needs full processing power of a powerful computer
Log Reviews	• Provides excellent information • Only data source that provides historical information	• Cumbersome to review • Automated tools not perfect can filter out important information
File Integrity Checkers	• Reliable method of determining whether a host has been compromised • Highly automated • Low cost	• Does not detect any compromise prior to installation • Checksums need to be updated when system is updated
Malicious Code Detectors	• Excellent at preventing and removing viruses •Low/Medium cost	• Require constant updates to be effective • Server based versions may have significant impact on performance • Some false positive issues • Ability to react to new, fast replicating viruses is often limited
War Dialing	• Effective way to identify unauthorized modems	• Legal and regulatory issues especially if using public switched network • Slow

Table D-4 describes a general schedule and list of evaluation factors for testing categories. Category 1 systems are those sensitive systems that provide security for the organization or that provide other important functions. These systems would include:

- Firewalls, routers, and perimeter defense systems such as for intrusion detection
- Public access systems such as web and email servers
- DNS and directory servers
- Other internal systems that would likely be intruder targets

Category 2 systems are generally all other systems, i.e., those systems that are protected by firewalls, etc., but that still must be tested periodically.

Table D-4. Summarized Evaluation Factors

Test Type	Category 1 Frequency	Category 2 Frequency	Complexity	Level of Effort	Risk	Benefit
Network Mapping	Quarterly	Annually Medium	High	Medium	Medium	• Enumerates the network structure and determines the set of active hosts, and associated software • Identifies unauthorized hosts connected to a network • Identifies open ports • Identifies unauthorized services
Vulnerability Scanning	Quarterly or bimonthly	Annually	High	High	Medium	• Enumerates the network structure and determines the set of active hosts, and associated software • Identifies a target set of computers to focus vulnerability analysis • Identifies potential vulnerabilities on the target set • Validates that operating systems and major applications are up to date with security patches and software versions
Penetration Testing	Annually	Annually	High	High	High	• Determines how vulnerable an organization's network is to penetration and the level of damage that can be incurred • Tests IT staff's response to perceived security incidents and their knowledge of and implementation of the organization's security policy and system's security requirements
Security Testing and Evaluation	At least every 3 years or when significant changes	At least every 3 years	High	High	High	• Uncovers design, implementation, and operational flaws that could allow the violation of security policy • Determines the adequacy of security mechanisms, assurances, and other properties to enforce the security policy • Assesses the degree of consistency between system documentation and implementation

Test Type	Category 1 Frequency	Category 2 Frequency	Complexity	Level of Effort	Risk	Benefit
Password Cracking	Monthly	Yearly	Low	Low	Low	• Verifies that the policy is effective in producing passwords that are more or less difficult to break • Verifies that users select passwords that are compliant with the organization's security policy
Log Reviews	Weekly	Weekly	Medium	Medium	Low	• Validates that the system is operating according to policies
Integrity Checkers	Monthly and in case of suspected incident	Monthly	Low	Low	Low	• Detects unauthorized file modifications
Malicious Code Detectors	Weekly or as required	Weekly or as required	Low	Low	Low	• Detects and deletes malicious code before successful installation on the system
War Dialing	Annually	Annually	Low	Low	Medium	• Detects unauthorized modems and prevents unauthorized access to a protected network

D.10 Operational System Auditing

Routine, independent reviews of security systems and procedures not only ensure an organization has adequate protections in place, but confirm that they are working as designed-and that employees are using them effectively.

Auditing is the mechanism that management can use to ensure the FAA's information is guarded effectively, that employees are adhering to policies and procedures, and that new products and services are incorporating security into their basic design. Auditors are not ubiquitous inspectors that delve into every nook and cranny of an organization's systems. Rather, an auditor will examine select policies, procedures and functions for individual system performance, or conduct a series of select reviews and extrapolate the results to develop an overall picture of the organization's security posture. Effective auditing requires technical competence.

D.10.1 Standards of Measure

Auditors will often use the same tools and methodologies as penetration testers and assessors when conducting a review of systems and procedures. It makes sense for an auditor to test an organization's perimeter to ensure that the firewall is strong, or that databases are appropriately segregated from the web server. The difference between auditing and other security evaluations is that it measures the outcome against prescribed standards of performance.

There is no one standard for electronic or physical security. Even the smallest organization will have multiple physical and technical security systems, making specific standards applicable only to specific applications, policies and processes.

The yardstick used by auditors can be anything from the performance expectation of an organization to government regulations to generally accepted industry standards. If managers want to know the effectiveness of the company's password-protection policy, for instance, the standard of measurement would be the number of employees adhering to and violating the policy. For applications such as authentication systems and firewalls, the audit could measure their effectiveness against the manufacturer's specifications.

Standards and measurements are critical to an audit. Without a baseline for gauging performance, there is no way an organization can judge the effectiveness of its systems or plot a course for improvement. Two broad classes of uses of standards and measurements can be identified as follows:

- **Decision support.** This is the primary use of most standards and measurements. Assessments of security properties are used to aid different kinds of decision making, such as risk management, resource allocation, program planning, or selection of specific products or services.
- **Mandated reporting of IS status or posture.** Organizations also use and define standards and measurements to respond to external demands. Reporting can be mandated to determine compliance with requirements, serve as a basis for trend analysis, or justify requests for additional resources. Specific metrics can be mandated; however, usually the reporting organization identifies the need for metrics to provide a succinct reporting mechanism.

D.10.2 Metrics

Several general problems with metrics can be identified:

- Metrics are often ill defined; consequently, any definition of a metric should include a specification of the process used to construct and evaluate it.

- The definition and evaluation of metrics frequently become distanced from the ultimate use, so that metrics become ends in themselves. That is, the consumer of the metric is lost in the definition of the metric.
- Metrics are often used or reported in contexts other than those for which they were originally intended.

A summary of the current state-of-the-art follows:

- No single metric will successfully quantify the assurance present in a system. The problem is far more complicated than that and the stakeholder community is much too diverse. Multiple measures will most certainly be applied and they will need to be refreshed frequently.
- Software and systems engineering are very much related to this problem. The quality of the software delivered, the architectures and designs chosen, the tools used to build systems, the specified requirements, and other topics are all related to the assurance we try to quantify.
- Penetration testing is, today, a valid metric. It is imperfect and to some extent non-repeatable, but nonetheless it is used in both government and commercial sectors. Several metrics relate to such testing: level of effort, number of vulnerabilities found, number of penetrations, and number of vulnerabilities not found.
- Defense in depth and breath is important. Knowing how to measure this defense is also important and is a related research area.
- Attempts to quantify and obtain a partial ordering of the security attributes of systems in the past have not been successful to a large degree. Examples are the *Trusted Computer System Evaluation Criteria* (TCSEC), Department of Defense (DoD) 5200.28-STD; and the *Common Criteria* (CC).
- Processes, procedures, tools, and people all interact to produce assurance in systems. Metrics that incorporate these aspects will remain critical to successful IT system operation.

The FAA should develop a set of metrics, policies, and procedures for auditing its ISS program. For example, see draft NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*.

D.10.3 Program and Compliance Reviews

Program and compliance reviews ensure that organizations are following applicable policy. There are two levels of reviews:

- **ISS Program Reviews.** These reviews ensure compliance with FAA Orders and policies and to collect information for evaluation of the FAA System for effectiveness and improvement.
- **IS Security Compliance Reviews.** These inspections examine whether the FAA System is meeting stated or implied security requirements, including system and organizational policies stated in the security plan. The inspection can also detect illegal acts, errors, irregularities, or a lack of compliance with laws, regulations, policy, and contracts.

Appendix E

Security Test Plan Template

Below is an example of a security test plan template from the *FAA Information Systems Security Program Handbook*, version 3. This template should be used as a guide in preparing a security test plan. This template may not meet the needs of all system test programs and may be tailored to satisfy the requirements of a system test program.

1. System Identification
   - Describe the function or purpose of the target system and information processed.
   - Describe the architecture of the system and include an architecture diagram.
2. System Test Environment
   - Describe in detail the system under test, including architectural drawings, descriptions of hardware and software, configuration, role within NAS, and criticality.
   - Describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources.
   - Include any security software protecting the system and information.
3. Test Team Composition
   - Identify the test organizations.
   - Describe the roles and responsibilities of the test organizations.
4. Test Resources
   - Describe the primary resources needed to perform the ISS test. Include hardware, software, and communications resources.
5. Security Test Description
   - Describe the scope of the ISS testing.
   - Provide a general description of the ISS tests. Include test objective, test method and success criteria.

6. Penetration Test Plan

   - Specific systems to be tested, including IP (and ATN, if applicable) addresses/ranges to be tested.
   - How intrusive the test will be.
   - The scope of testing (e.g., interfaces with other systems and how far into these systems testing will go).
   - Any restricted hosts (i.e., hosts, systems, subnets, not to be tested).
   - A list of acceptable testing techniques (e.g., social engineering, DoS) and tools (e.g., password crackers, network snifters).
   - The extent of testing (e.g., which level, or impact, of vulnerabilities will be exploited).
   - Times that scanning is to be conducted (e.g., during business hours, after business hours).
   - IP addresses of the machines from which penetration testing will be conducted so that administrators can differentiate the legitimate penetration testing attacks from actual hacker attacks.
   - Points of contact for both the penetration testing team and the targeted systems and networks.
   - Evidence that notice has been given to test conduits and consent has been obtained from test targets.
   - Measures to prevent law enforcement being called with false alarms.
   - Handling of information collected by penetration testing team.
   - Whether penetration testing is to be overt (Blue Teaming) or covert (Red Teaming).
   - Identification of trusted third party (if any), government test liaison, to assist with issues that arise during testing (e.g., scope, methodology, extent of exploiting).
   - If testing in a live or operational environment, an explanation why that is necessary and what less intrusive methods have been exhausted.

Appendix F

Security Test Plan Procedure Template

Below is an example of a security test procedure template. This template should be used as a guide in preparing a security test plan. This template may not meet the needs of all system test programs and may be tailored to satisfy the requirements of a particular FAA System security test.

Date:	
Host Name:	
Host Function:	
IP Address(es) If Applicable:	
Test Performed By:	
Test Name:	
Test Method:	
Assumptions:	
Prerequisite Tests:	
Security Requirement(s):	
Required Resources:	
Expected Results:	
Test Procedures:	
Tools Used:	
Documentation Used:	
Detailed Test Results (Please attach the results of any tests run, or refer to electronic file):	
TEST (Circle One) **PASSED** **FAILED**	

Appendix G

Security Test Report Template

Below is an example of a security test report template. This template should be used as a guide in preparing a security test plan. This template may not meet the needs of all system test programs and may be tailored to satisfy the requirements of a particular FAA System security test.

1. Executive Test Results Summary
    - Briefly summarize the results of the ISS testing, emphasizing any recommendations or special security concerns.
2. System Identification
    - Briefly describe the function or purpose of the target system and information processed.
3. Test Participants
    - List the test participants (e.g., test team members).
4. System Test Configuration
    - Briefly describe the system test configuration. Include primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources.
5. Description of Test Results
    - Describe in detail the results from the testing.
    - Describe any deviations from the planned testing.
6. Test Results Data
    - Include data that support the results.
    - Described the test results data.
    - Omit data that can be used to compromise the security of the system (e.g., passwords, IP addresses).

Appendix H

FAA System Security Specifications

Security specifications for the FAA System are expressed in the System Level Specification (SLS), or System Specification Document (SSD). The following specifications are typical. They are extracted from FAA Order 1370.82 and the *NAS System Protection Profile Template* (SPPT) version 1 and are expected to be incorporated in a Protection Profile written for a FAA System. When incorporated in a solicitation or contract, some of the security specifications may be merged with non-security specifications. In general the final specifications will be the union of the security and non-security specifications.

H.1 SLS Security Specifications

SLS 3.4 Security

FAA Order 1370.82 requires a Protection Profile for all FAA systems. The Protection Profile used for the FAA System is the FAA System Protection Profile.

SLS 3.4.1 Identification and Authentication

The FAA System shall provide the functional security requirement elements for identification and authentication as specified in the FAA System *Protection Profile,* Section 5.1 including: identification, authentication, authentication failures, user attribute definition and enforcing quality metrics on secrets.

Note: Identification and Authentication address functions to establish and verify a claimed identity. These functions are required to ensure that entities are associated with the proper Security Attributes (e.g., identity, groups, roles, security, or integrity levels).

Note: All authorized entities may be assigned a set of security attributes that may be used to enforce the FAA System Security Policy. User Attribute Definition defines the specifications for associating user security attributes with entities as needed to support the FAA System Security Policy.

Note: For example, a quality metric includes passwords which may be required to meet certain quality standards (i.e., 8 characters, mixed case).

SLS 3.4.2 Security Audit

The FAA System shall provide the functional security requirement elements for security audit generation as specified in the FAA System *Protection Profile* Section 5.2 including:

- Security Audit Data Generation
- Intrusion Identification Analysis

- Security Audit Review
- Security Audit Event Selection
- Security Audit Event Storage
- Operational Attack and Vulnerability Analysis and Remediation

Note: Security auditing involves recognizing, recording, storing, and analyzing information related to security relevant activities (i.e., activities controlled by the FAA System Security Policy). The resulting audit records may be examined to determine which security relevant activities have taken place and which entity is responsible for them.

Note: Intrusion Identification Analysis defines specifications for automated means that analyze system activity and audit log data looking for possible or real security violations.

SLS 3.4.3 Security Management

The FAA System shall provide the functional security requirement elements for security management as specified in the FAA System *Protection Profile* Section 5.3 including:

- Management of Security Functions Behavior
- Management of Security Attributes
- Management of FAA System Security Data
- User and Administrator Roles

SLS 3.4.4 Network Security Protection

The FAA System shall provide the functional security requirement elements for network security protection as specified in the FAA System *Protection Profile* Section 5.5.

Note: Network Security Protection addresses the responsibility for maintaining the overall security posture of the NAS by providing:

- Protection of network communications between FAA System and other FAA Systems
- Protection of network communications to security domains outside the FAA
- Countermeasures corresponding to special or unique vulnerabilities of the FAA System

SLS 3.4.5 Application Data Protection

The FAA System shall provide the functional security requirement elements for application data protection as specified in the FAA System *Protection Profile* Section 5.6 including:

- Access Control
- Information Flow Control
- Import from External Systems
- Export to External Systems

SLS 3.4.6 Protection of the FAA System Security Data and Mechanisms

The FAA System shall provide the functional security requirement elements for protection of the FAA System and mechanisms as specified in the FAA System *Protection Profile* Section 5.7 including:

- Internal FAA System Data Transfer
- Tamper Protection
- Security Policy Enforcement Modularity and Continuity
- Trusted Recovery
- Reference Mediation
- Domain Separation
- Time Stamps
- FAA System Self Test

Note: Protection of the FAA System Security Data and Mechanisms addresses the integrity and management of the data and mechanisms that implement the FAA System Security Policy.

Note: Trusted recovery ensures that the FAA System can determine that it has started up without protection compromise and can recover without protection compromise after discontinuity of operations. Trusted Recovery also addresses the consistency of data that implement the FAA System Security Policy after discontinuity or interruption of communication of and among FAA System components.

SLS 3.4.7 Resource Utilization

The FAA System shall provide the functional security requirement elements for resource utilization as specified in the FAA System *Protection Profile* Section 5.8 including:

- Priority of Service
- Resource Allocation

SLS 3.4.8 FAA System Access

The FAA System shall provide the functional security requirement elements for FAA System access as specified in the FAA System *Protection Profile* Section 5.9 including:

- Limitation on Scope of Selectable Attributes
- Limitation on Multiple Concurrent Sessions
- Session Locking
- Access Banners
- Access History
- Session Establishment

SLS 3.4.9 Trusted Path

The FAA System shall provide the functional security requirement elements for trusted paths as specified in the FAA System *Protection Profile* Section 5.10.

Note: A trusted path provides confidence that a user is communicating directly with the FAA System whenever it is invoked. A user's response via the trusted path guarantees that untrusted applications cannot intercept or modify the user's response.

SLS 3.4.10 Configuration Management (CM)

The FAA System shall provide the functional security requirement elements for configuration management as specified in the FAA System *Protection Profile* Section 6.2.

Note: CM systems are put in place to ensure the integrity of the portions of the FAA System that they control, by providing a method of tracking any changes, and by ensuring that all changes are authorized.

SLS 3.4.11 Data Management

The FAA System shall provide for the management for data in accordance with FAA Order 1375.1C, *Data Management* and FAA Order 1200.22C, *NAS Data and Interface Equipment Used by Outside Interests.*

SLS 3.4.12 Internet Access

The FAA System shall protect any access to the Internet in accordance with FAA Order 1370.83, *Internet Access Points* and FAA Order 1370.84 *Internet Services.*

H.2 SOW and DID Security Specifications

The following SOW and DID elements are extracted from the *NAS SPPT*. When the CC prescribes additional evaluator action elements, they are also quoted. These elements are

expected to be incorporated in the Protection Profile written for the FAA System. Some of these elements will be part of non-security-related specifications. These elements were written as part of the *NAS SPPT* for completeness. However, when the *SPPT* is incorporated into a solicitation document, the specifications may be subsumed elsewhere than the security section.

SPPT 5.1.2. Authentication

Statement of Work Elements

a. The developer shall perform necessary analysis and recommend authentication mechanisms suitable for FAA System needs.

SPPT 5.1.4. User Attribute Definition

Statement of Work Elements

a. The developer shall recommend the multiple security attributes that could be associated with individual entities necessary for the FAA System's needs.

b. The developer shall perform necessary analysis and recommend COTS products implementing the multiple security attributes employed by the FAA System.

SPPT 5.2.2. Intrusion Identification Analysis

Statement of Work Elements

a. The developer shall conduct a survey of the COTS product capabilities, perform necessary analysis, and recommend host-based, server-based, network-based, and hybrid intrusion identification tools suitable for FAA System needs.

b. The developer shall conduct a survey of the COTS product capabilities, perform necessary analysis, and recommend a combination of host-based, server-based, network-based, and hybrid automated intrusion identification tools suitable for FAA System needs with consideration of NAS-wide intrusion detection services.

SPPT 5.2.6. Operational Attack and Vulnerability Analysis and Remediation

Statement of Work Elements

a. The developer shall conduct a survey of available product capabilities, perform necessary analysis, and recommend host-based, server based, network-based, and hybrid automated operational vulnerability analysis and remediation tools with which to perform and document an analysis of ways in which the FAA System security policy could be violated. Tools include, but are not limited to, detection and remediation of: viruses and other malicious code, published vulnerabilities, insecure configuration, and unauthorized change.

SPPT 5.4.1. Key Management Cryptographic Support

Statement of Work Elements

a. The developer shall: conduct a survey of COTS cryptographic product capabilities and standards, including standards from NIST (including but not limited to FIPS 140-2, June 2001, *Security Requirements for Cryptographic Modules*; FIPS 180-1, April 1995, *Secure Hash Standard*; FIPS 186-2, January 2000, *Digital Signature Standard (DSS)*), ISO, IETF, ICAO, and industry groups; perform necessary analysis; and recommend a cryptographic algorithm or algorithms to be used by the FAA System, interoperate with security domains outside the FAA, and interoperate with other FAA Systems, as required.

SPPT 5.5.1. FAA System Protection

Statement of Work Elements

a. The developer shall conduct a survey of COTS product capabilities, perform necessary analysis, and recommend a security architecture including procedures and technology to counter special or unique vulnerabilities of the FAA System, communications to security domains outside the FAA, and communications among FAA Systems.

SPPT 6.1.1. FAA System Security Description

Statement of Work Elements

a. The developer shall provide a description of the security properties of the FAA System.

Data Item Description Elements

b. The description of the security properties of the FAA System shall, as a minimum, describe the security and non-security services provided by the FAA System, and the scope and boundaries of the FAA System in general terms both in a physical and a logical way.

SPPT 6.1.2. FAA System Security Environment

Statement of Work Elements

a. The developer shall provide a statement of the FAA System security environment.

Data Item Description Elements

b. The statement of the FAA System security environment shall identify and explain any assumptions about the intended usage of the FAA System and the environment in which is intended to be used.

c. The statement of the FAA System security environment shall identify and explain any known or presumed threats to the assets against which protection will be required, either by the FAA System or by its environment.

d. The statement of the FAA System security environment shall identify and explain any organizational security policies with which the FAA System must comply.

e. The statement of the FAA System security environment shall identify and explain the threats originating in systems external to the FAA security domain.

f. The statement of the FAA System security environment shall identify and explain the architecture, design, protocols, and use of interfaces between the FAA System and other (sub)systems within the FAA security domain as well as systems external to the FAA security domain.

SPPT 6.1.3. Allocation of Security Objectives

Statement of Work Elements

a. The developer shall provide a statement of security objectives allocation.

b. The developer shall provide the security objectives allocation rationale.

Data Item Description Elements

c. The statement of security objectives shall define the security objectives for the FAA System and its environment.

d. The security objectives for the FAA System shall be clearly stated and traced back to aspects of the identified threats to be countered by the FAA System technology and/or organizational security policies to be met by the FAA System technology.

e. The security objectives for the environment shall be clearly stated, allocated to physical or procedural measures, and traced back to aspects of identified threats not completely countered by the FAA System technology and/or organizational security policies or assumptions not completely met by the FAA System technology.

f. The security objectives rationale shall demonstrate that the stated security objectives are suitable to counter the identified threats to security.

g. The security objectives rationale shall demonstrate that the stated security objectives are suitable to cover all of the identified organizational security policies and assumptions.

SPPT 6.1.4. FAA System Security Summary Specification

Statement of Work Elements

a. The developer shall provide FAA System Functional Security Specifications.

b. The developer shall provide the FAA System Functional Security Specifications rationale.

Data Item Description Elements

c. The FAA System Functional Security Specifications shall describe the IT security functions and the assurance measures of the FAA System.

d. The security functions shall be defined in an informal style to a level of detail necessary for understanding their intent.

e. All references to security mechanisms provided by the developer, or to environmental or procedural mechanisms assumed or recommended by the developer, shall be traced to the relevant FAA System Functional Security Specifications so that it can be seen which security mechanisms are used in the implementation of each function.

f. The FAA System Summary Specification rationale shall demonstrate that the security functions are suitable to meet the FAA System Functional Security Specifications.

g. The FAA System Functional Security Specifications rationale shall demonstrate that the combination of the specified security functions work together so as to satisfy the FAA System Functional Security Specifications.

h. The FAA System Functional Security Specifications shall trace the assurance measures to the assurance specifications so that it can be seen which measures contribute to the satisfaction of which specifications.

i. The FAA System Functional Security Specifications rationale shall justify how the assurance measures meet all assurance specifications of the FAA System.

j. The FAA System Functional Security Specifications shall identify all IT security functions that are realized (implemented) by a probabilistic or permutational mechanism, as appropriate.

k. The FAA System Functional Security Specifications shall, for each IT security function for which it is appropriate, state the strength of function as a specific metric.

SPPT 6.2.1. CM Automation

Statement of Work Elements

a. The developer shall use a CM system.

b. The developer shall provide a CM plan.

c. The developer shall deliver to the FAA the CM system complete with all data necessary for the FAA to continue to use the CM system for NAS Subsystem. Delivery of the CM data shall accompany delivery of each version of NAS Subsystem to the FAA and at termination of this contract.

Data Item Description Elements

d. The CM system shall provide an automated means by which only authorized changes are made to the NAS Subsystem implementation.

e. The CM system shall provide an automated means to support the generation of the NAS Subsystem.

f. The CM plan shall describe the automated tools used in the CM system.

g. The CM plan shall describe how the automated tools are used in the CM system.

SPPT 6.2.2. CM Capabilities

Statement of Work Elements

a. The developer shall use a CM system.

b. The developer shall provide a reference for each specific release of the NAS Subsystem implementation.

c. The developer shall provide CM documentation.

Data Item Description Elements

d. The reference for the NAS Subsystem shall be unique to each version of the NAS Subsystem.

e. The NAS Subsystem shall be labeled with its reference as specified in *b.* above.

f. The CM documentation shall include a configuration list and configuration plan.

g. The configuration list shall describe the configuration items that comprise the NAS Subsystem.

h. The CM documentation shall describe the method used to uniquely identify the configuration items.

i. The CM system shall uniquely identify all configuration items.

j. The CM plan shall describe how the CM system is used.

k. The CM system shall provide measures such that only authorized changes are made to the configuration items.

SPPT 6.3.1. Delivery

Statement of Work Elements

a. The developer shall document procedures for delivery of FAA System or parts of it to the FAA.

b. The developer shall use the delivery procedures.

Data Item Description Elements

c. The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of FAA System to the FAA.

SPPT 6.3.2. Installation, Generation, and Start-up Procedures

Statement of Work Elements

a. The developer shall document procedures necessary for the secure installation, generation, and start-up of the FAA System.

Data Item Description Elements

b. The documentation shall describe the steps necessary for secure installation, generation, and start-up of the FAA System.

Additional Evaluator Action Elements

c. The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

SPPT 6.4.1. FAA System Functional Security Specification

Statement of Work Elements

a. The developer shall provide a functional security specification.

Data Item Description Elements

b. The functional security specification shall describe the security properties of the FAA System and its external interfaces using an informal style.

c. The functional security specification shall be internally consistent.

d. The functional security specification shall describe the security properties including purpose and method of use of all external FAA System interfaces, providing details of effects, exceptions, and error messages.

e. The functional security specification shall completely represent the security properties of the FAA System.

Additional Evaluator Action Elements

f. The evaluator shall determine that the functional specification is an accurate and complete instantiation of the FAA System security functional requirements.

SPPT 6.4.2. Descriptive High-Level Security Design

Statement of Work Elements

a. The developer shall provide the high-level design of the security properties of the FAA System.

Data Item Description Elements

b. The presentation of the high-level design shall be informal.

c. The high-level design shall be internally consistent.

d. The high-level design shall describe the structure of the security properties of the FAA System in terms of subsystems.

e. The high-level design shall describe the security functionality provided by each subsystem of the FAA System.

f. The high-level design shall identify any underlying hardware, firmware, software, and/or communications required by the FAA System with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, software, and/or communications.

g. The high-level design shall identify all interfaces to the security-relevant subsystems of the FAA System.

h. The high-level design shall identify which of the interfaces to the subsystems of the FAA System are externally visible.

i. The high-level design shall include a description of the FAA System defense-in-depth, identifying how the combination of technical and non-technical countermeasures reduce the level of residual risk to an acceptable level.

Additional Evaluator Action Elements

j. The evaluator shall determine that the high-level design is an accurate and complete instantiation of the FAA System security functional requirements.

SPPT 6.4.3. FAA System Functional Specification

The development of FAA System functional specifications is an item that a developer will do as part of the normal contract. The following elements from the PP template may be superfluous or may add to the specificity of the DID.

Statement of Work Elements

a. The developer shall provide a functional specification.

Data Item Description Elements

b. The functional specification shall describe the non-security-relevant functions performed by the FAA System using an informal style.

c. The functional specification shall be internally consistent.

d. The functional specification shall describe the purpose and method of use of all external interfaces and protocols, providing details of effects, exceptions, and error messages.

e. The functional security specification shall completely represent the functions performed by the FAA System.

Additional Evaluator Action Elements

f. The evaluator shall determine that the functional specification is an accurate and complete instantiation of the FAA System non-security-relevant functions.

SPPT 6.4.4. Descriptive High-Level Functional Design

Statement of Work Elements

a. The developer shall provide the high-level functional design of the functions performed by the FAA System.

Data Item Description Elements

b. The presentation of the high-level functional design shall be informal.

c. The high-level functional design shall be internally consistent.

d. The high-level functional design shall describe the structure of the FAA System in terms of subsystems.

e. The high-level functional design shall describe the functionality provided by each subsystem of the FAA System.

f. The high-level functional design shall identify any underlying hardware, firmware, software, and/or communications required by the FAA System with a presentation of

the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, software, and/or communications.

g. The high-level functional design shall identify all interfaces to the security-relevant subsystems of the FAA System.

h. The high-level functional design shall identify which of the interfaces to the subsystems of the FAA System are externally visible.

i. The high-level functional design shall identify the purpose and utilization of all connections to external interfaces and the protocols employed.

j. The high-level design shall include a description of the FAA System defense-in-depth, identifying how the combination of technical and non-technical countermeasures reduce the level of residual risk to an acceptable level.

Additional Evaluator Action Elements

k. The evaluator shall determine that the high-level functional design is an accurate and complete instantiation of the FAA System non-security-relevant functional requirements.

SPPT 6.5.1. Security Administrator Guidance

Statement of Work Elements

a. The developer shall provide administrator guidance addressed to system administrative personnel.

Data Item Description Elements

b. The security administrator guidance shall describe the administrative functions and interfaces available to the FAA System administrator.

c. The security administrator guidance shall describe how to administer the FAA System in a secure manner.

d. The security administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

e. The security administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the FAA System.

f. The security administrator guidance shall describe all security parameters under the control of the security administrator, indicating secure values as appropriate.

g. The security administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the FAA System.

h. The security administrator guidance shall be consistent with all other documentation supplied.

i. The security administrator guidance shall describe all security specifications for the IT environment that are relevant to the security administrator.

SPPT 6.5.2. User Guidance

Statement of Work Elements

a. The developer shall provide user guidance.

Data Item Description Elements

b. The user guidance shall describe the functions and interfaces available to the non-administrative users of the FAA System.

c. The user guidance shall describe the use of user-accessible security functions provided by the FAA System.

d. The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

e. The user guidance shall clearly present all user responsibilities necessary for secure operation of the FAA System, including those related to assumptions regarding user behavior found in the statement of the FAA System security environment.

f. The user guidance shall be consistent with all other documentation supplied.

SPPT 6.6.1. Development Security

Statement of Work Elements

a. The developer shall produce development security documentation.

Data Item Description Elements

b. The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the FAA System design and implementation in its development environment.

c. The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the FAA System.

Additional Evaluator Action Elements

d. The evaluator shall confirm that the security measures are being applied.

SPPT 6.6.2. Flaw Remediation

Statement of Work Elements

a. The developer shall document the flaw remediation procedures.

b. The developer shall establish a procedure for accepting and acting upon reports of security flaws and requests for corrections to those flaws.

Data Item Description Elements

c. The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the FAA System.

d. The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

e. The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

f. The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections, and guidance on corrective actions to the FAA.

g. The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to the FAA.

h. The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

SPPT 6.6.3. Life Cycle Definition

Statement of Work Elements

a. The developer shall establish a life-cycle model to be used in the development and maintenance of the FAA System.

b. The developer shall provide life-cycle definition documentation.

c. The developer shall use the ESP model to develop and maintain the FAA System.

Data Item Description Elements

d. The life-cycle definition documentation shall describe the model used to develop and maintain the FAA System.

e. The life-cycle model shall provide for the necessary control over the development and maintenance of the FAA System.

f. The life-cycle definition documentation shall explain why the model was chosen.

g. The life-cycle definition documentation shall explain how the ESP model is used to develop and maintain the FAA System.

h. The life-cycle definition documentation shall demonstrate compliance with the ESP life-cycle model.

SPPT 6.7.1. Assurance Maintenance Plan

Statement of Work Elements

a. The developer shall provide an Assurance Maintenance Plan.

Data Item Description Elements

b. The Assurance Maintenance Plan shall contain or reference a brief description of the FAA System, including the security functionality it provides.

c. The Assurance Maintenance Plan shall identify the baseline version of the FAA System by its unique CM reference.

d. The Assurance Maintenance Plan shall define the scope of changes to the FAA System that are covered by the plan.

e. The Assurance Maintenance Plan shall describe the FAA System life cycle, and shall identify the current plans for any new releases of the FAA System, together with a brief description of any planned changes that are likely to have a significant security impact.

f. The Assurance Maintenance Plan shall describe the assurance maintenance cycle, stating and justifying the planned schedule.

g. The Assurance Maintenance Plan shall describe how the developer will ensure that the procedures documented or referenced in the Assurance Maintenance Plan are followed.

h. The Assurance Maintenance Plan shall describe how the developer will ensure that all developer actions involved in the analysis of the security impact of changes affecting the FAA System are performed correctly.

i. The Assurance Maintenance Plan shall describe or reference the procedures to be applied to maintain the assurance in the FAA System, which as a minimum shall include the procedures for configuration management, maintenance of assurance evidence, performance of the analysis of the security impact of changes affecting the FAA System, and flaw remediation.

Additional Evaluator Action Elements

j. The evaluator shall confirm that the proposed schedules for Assurance Maintenance audits and reevaluation of the FAA System are acceptable and consistent with the proposed changes to the FAA System.

SPPT 6.7.2. Evidence of Assurance Maintenance

Statement of Work Elements

a. The developer shall provide Assurance Maintenance documentation for the current version of the FAA System.

Data Item Description Elements

b. The Assurance Maintenance documentation shall include a configuration list and a list of identified vulnerabilities in the current version of the FAA System.

c. The configuration list shall describe the configuration items that comprise the current version of the FAA System.

d. The list of identified vulnerabilities in the current version of the FAA System shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the FAA System.

e. The Assurance Maintenance documentation shall provide evidence that the procedures documented or referenced in the Assurance Maintenance Plan are being followed.

f. The Assurance Maintenance documentation shall provide evidence that functional testing has been performed, on the current version of the FAA System, to a degree commensurate with the level of assurance being maintained.

Additional Evaluator Action Elements

g. The evaluator shall confirm that the procedures documented or referenced in the Assurance Maintenance Plan are being followed.

h. The evaluator shall confirm that the security impact analysis for the current version of the FAA System is consistent with the configuration list.

i. The evaluator shall confirm that all changes documented in the security impact analysis for the current version of the FAA System are within the scope of changes covered by the Assurance Maintenance Plan.

j. The evaluator shall confirm that functional testing has been performed on the current version of the FAA System, to a degree commensurate with the level of assurance being maintained.

SPPT 6.7.3. Security Impact Analysis

Statement of Work Elements

a. The developer shall, for the current version of the FAA System, provide a security impact analysis that covers all changes affecting the FAA System as compared with the baselined version.

Data Item Description Elements

b. The security impact analysis shall identify the baselined FAA System by its unique CM reference from which the current version of the FAA System was derived.

c. The security impact analysis shall identify all new and modified FAA System components that are categorized as security policy-enforcing.

d. The security impact analysis shall, for each change, identify all IT security functions and all FAA System components categorized as security policy-enforcing that are affected by the change.

e. The security impact analysis shall, for each change that results in a modification of the implementation, identify the test evidence that shows, to the required level of assurance, that the trusted security function continues to be correctly implemented following the change.

f. The security impact analysis shall, for each applicable assurance specification in the configuration management, life cycle support, delivery, and operation and guidance documents assurance specifications, identify any deliverables that have changed and provide a brief description of each change and its impact on assurance.

g. The security impact analysis shall, for each applicable assurance specification in the vulnerability assessment assurance specifications, identify which deliverables have changed and which have not, and give reasons for the decision taken as to whether or not to update the deliverable.

Additional Evaluator Action Elements

h. The evaluator shall check, by sampling, that the security impact analysis documents changes to an appropriate level of detail, together with appropriate justifications that assurance has been maintained in the current version of the FAA System.

SPPT 6.9.1. Strength of Security Functions

Statement of Work Elements

a. The developer shall perform a strength of security function analysis for each mechanism having a strength of security function specification.

Data Item Description Elements

b. The strength of security function analysis shall show compliance or non-compliance with all applicable regulations, including but not limited to: FIPS 190 *Guidelines for the Use of Advanced Authentication Technology Alternatives*, FIPS 74 *Guidelines for Implementing and Using the NBS Data Encryption Standard (DES)*, FIPS 112 *Password Usage*, and, when issued, the FIPS for the Advanced Encryption System (AES).

Additional Evaluator Action Elements

c. The evaluator shall confirm that the strength claims are correct.

SPPT 6.9.2. Developer Vulnerability Analysis

Statement of Work Elements

a. The developer shall perform and document an analysis of the FAA System and all other deliverables searching for ways in which a user can violate the Security Policy of this or any other FAA System.

b. The developer shall document the disposition of vulnerabilities identified as part of Developer Vulnerability Analysis.

c. The developer shall document the disposition of vulnerabilities identified as part of Independent Vulnerability Analysis.

d. The analysis shall incorporate the statement of the FAA System security environment developed specified in Section **b**, including the threats originating in systems external to the FAA security domain.

Data Item Description Elements

e. The documentation shall show, for all vulnerabilities identified by the Developer Vulnerability Analysis or Independent Vulnerability Analysis, whether the vulnerability can or cannot be exploited in the FAA System as installed and used; or, as part of the high-level design of the FAA System defense-in-depth, identify how the combination of technical and non-technical countermeasures reduce the level of residual risk to an acceptable level.

f. The documentation shall justify that the FAA System, with the identified vulnerabilities, is resistant to published and other well-known and obvious vulnerabilities and flaws.

g. The evidence shall show whether the search for vulnerabilities is systematic.

h. The evidence shall show whether identified vulnerabilities attributable to the architecture, design, protocols, and use of interfaces between this FAA System and

other FAA Systems, and between the FAA System and systems external to the FAA security domain, will or will not enable violation of the Security Policy of this or any other FAA System or decrease the security posture of the set of all the FAA Systems.

Additional Evaluator Action Elements

i. The evaluator shall perform an independent vulnerability analysis. See *NAS Protection Profile Template* Section 5.7.4 Independent Test Actions and Specifications.

j. The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.

k. The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.

Glossary

A&MS	Administrative and Mission Support
ACB	Innovations & Solutions
AF	Airway Facilities
ARTCC	Air Route Traffic Control Center
AIS	Information Security
AMS	Acquisition Management System
AOS	Operational Support Service
APB	Acquisition Program Bulletin
ASP	Acquisition Strategy Paper
AT	Air Traffic
ATN	Aeronautical Telecommunications Network
ATS	Air Traffic Services
BIS	Boundary Intermediate System
C&A	Certification and Authorization (or Accreditation
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratories
CDRL	Contract Data Requirements List
CEM	Common Evaluation Methodology
CLNP	Connectionless Network Protocol
CM	Configuration Management
CMA	Context Management Application
COI	Critical Operational Issue
COTS	Commercial-Off-the-Shelf
CSC	Computer Science Corporation
DAA	Designated Approving Authority
DID	Data Item Description
DISA	Defense Information Systems Agency
DLAP	Data Link Applications Processors
DR&A	Data Reduction and Analysis
DT	Development Test
EAL	Evaluation Assurance Level
FAA	Federal Aviation Administration
FAST	FAA Acquisition System Toolset

FIPS	Federal Information processing Standard
HID	HCS Interface Device
HNL	HID/NAS LAN
ICAO	International Civil Aviation Organization
IETF	Internet Engineering Task Force
IOT&E	Independent Operational Test and Evaluation
IP	Internet Protocol
IPSec	Internet Protocol Security
IPP	Integrated Program Plan
IPT	Integrated Product Team
ISM	In-Service Management
ISS	Information System Security
ISSA	Information System Security Architecture
ISSM	Information System Security Manager
IT	Information Technology
IV&V	Independent Validation and Verification
JRC	Joint Resources Council
LAN	Local Area Network
M&C	Monitor and Control
NAS	National Airspace System
NIACAP	National Information Assurance Certification and Accreditation Process
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCD	Operational Capability Demonstration
OCT	Operational Capability Test
OKC	Oklahoma City
OSI	Open System Interconnection
OT	Operational Test
OT&E	Operational Test and Evaluation
PAT	Production Acceptance Test
PP	Protection Profile
PT	Penetration Test

PTR	Program Trouble Report
RD	Requirements Document
SARPs	Standards and Recommended Practices
SCAP	Security Certification and Authorization Package
SDNS	Secure Data Network System
SI	Solution Implementation
SLS	System Level Specification
SOW	Statement of Work
SP3	SDNS Security Protocol 3 for the OSI Network Layer
SP4	SDNS Security Protocol 4 for the OSI Transport Layer
SPPT	System Protection Profile Template
SRD	System Requirements Document
SSD	System Specification Document
SSS	System Subsystem Specifications
ST&E	Security Testing and Evaluation
TCP	Transmission Control Protocol
T&E	Test and Evaluation
TOE	Target of Evaluation
VA	Vulnerability Assessment
VPN	Virtual Private Network
WJHTC	William J. Hughes Technical Center