Appendix S

Security Engineering Plan Template

This page is intentionally left blank.

Title Page
Document Control Panel
Table of Contents
List of Acronyms
Definitions

1. General

Security engineering is a discipline that focuses on the tools, processes, and methods required to design, implement, and test systems that remain dependable in the face of malice, error, or misfortune. In the context of ITS, it is about ensuring that the control and monitoring of transportation infrastructure continues unimpeded despite malicious attacks, human errors, or natural disasters. Since the transportation infrastructure is vital to commerce, public safety, and national defense, it is imperative that the infrastructure be designed and built to survive threats against it. With the increasing use of (and dependency on) computer technology comes new vulnerabilities to the transportation infrastructure to intentional and unintentional threats. Since ITS is principally networked computer systems and sensors, security engineering should focus on processes and methods to protect networks, computer systems (i.e., hardware and software), and data. These areas are generally addressed under the umbrella of information security. Awareness and practice of information security is imperative to maintain the availability of our transportation systems in light of new technologies and new threats.

This document is intended to provide guidance for overall FDOT ITS security engineering processes as well as a template for tailoring project-specific security engineering plans.

1.1 Scope

Security engineering methodologies need to be applied pervasively throughout an organization and project to be effective. Security cannot be "bolted on" to a design with anywhere near the success of a design that was engineered with security in mind throughout the engineering process. One of the primary failings with bolt-on approaches is the lack of defense in depth. Without security engineering throughout a design, the entire system is potentially vulnerable if the external countermeasure is compromised. Similarly, focusing security awareness in only a portion of the engineering organization will likely result in the security mechanisms being applied topically, rather than integrated in the design.

From a project life-cycle perspective, it is important to consider security issues and practices during all phases of the project life cycle. Ignoring security issues during the requirements analysis or design phases will result in costly rework or less effective external solutions to meet security certification requirements that arise prior to deployment. It is vital to think of security engineering as an integrated discipline in the SEP. It can be significantly more expense (and have severe schedule impacts) to attempt to remediate security issues late in the project life cycle.

Similarly, it is important to distribute awareness and practice of security engineering across the organization. Concentrating all responsibility for design, implementation, and testing of security-related functionality in a specialized organization or individual will not yield a robust solution. Security engineering affects all engineering disciplines and responsibility should be distributed across the engineering organization. Section 2 of this document discusses the role of security engineering within the engineering organization in more detail.

The final dimension of the security engineering scope to consider is project type. Since security engineering is partly based on risk analysis, it is logical to assume that projects might require varying degrees and applications of security engineering. There is some truth to this assumption, although the very nature of the ITS domain is such that it is difficult to imagine many ITS-related projects that would not need to address security. The fact that ITS is inherently a distributed system with many touch points exposed to the public makes it particularly vulnerable. The trend of providing public access to transportation information technology (IT) via the Internet and advances with intelligent vehicles also increases the risk over traditional interfaces, such as signaling devices and sensors.

1.2 Security Engineering Approach

Security engineering is fundamentally risk management – identifying potential risks and determining practical solutions to prevent/protect the system against those risks. This process has been formalized (largely by the USDoD) into the threat-vulnerability-countermeasures methodology. With this process, one identifies potential threats to the system, analyzes the system to determine vulnerabilities to the threats, and then designs countermeasures to mitigate the vulnerabilities to the threats. The hidden challenge in this process is determining the extent to which each identified vulnerability should be addressed. It is usually impractical, both from an affordability and operational impact standpoint, to totally address all vulnerabilities in a system. The goal is to assess the impact to the system mission, along with the probability of the threat, and design countermeasures whose cost and impact to system operation is proportional. A popular axiom in information security is that the only completely secure system is one that doesn't do anything. The approach should be to minimize the risks that are most likely to occur, not protect against any conceivable threat.

This process should start early in the project life cycle. Threat analysis should typically be part of the concept of operations (ConOps) analysis, as well as the system requirements process. Threats should be viewed as part of the system's operational context. Vulnerabilities and countermeasures should be integral considerations to the design and implementation of a system, and security evaluation/accreditation must obviously be part of the system integration and testing (SIT) phase. In fact, the security engineering process should be part of the postengineering operation phase so that the system can be potentially enhanced to meet emerging threats not foreseen during the design phase.

Another aspect of the recommended ITS security engineering approach is the incremental adoption of process based on both project vulnerability and organization maturity. It is impractical to expect an organization to immediately institute every aspect of a complete security engineering process without the appropriate training and experience.

All of these areas will be covered in greater detail in subsequent sections of this document.

2. Security Engineering Administration

2.1 Organizational Structure Overview

The greatest asset in creating and operating a secure system is awareness by the designers, operators, and users. To this end, it is recommended that the FDOT adopt security engineering as a core engineering value that is promoted throughout the engineering organization. While some specialized personnel will be appropriate, the most effective security solution is one where all of the engineering disciplines participate. Engineering management should ensure that security concerns are included in the criteria used to assess the quality and completeness of all ITS projects.

While most of the actual security engineering effort will be performed by the engineers tasked with the design and implementation of the system, FDOT ITS projects should have a person responsible for ensuring the quality and compliance of the security engineering work performed, as well as providing domain expertise. This is a specialty engineering role similar to safety engineering; reliability and maintainability (R&M) engineering; and human factors engineering (HFE). It is recommended that this individual (and staff, if necessary) report to the project's systems engineering organization.

In addition, it is recommended that the FDOT establish a central security engineering organization to be staffed by individuals with training and expertise in security engineering. This organization should be responsible for the FDOT's security engineering policy and procedures, as well as providing technical expertise to projects as required.

2.2 Security Engineering Organization

As mentioned in *Section 2.1* of this appendix, the FDOT should create a security engineering organization to support all ITS projects, as well as provide domain governance via policy and procedures. The makeup of this organization should initially be a working group of systems and software engineers supplemented by subcontracted domain experts, with the goal of creating an FDOT staff of trained security engineers. The specific roles and responsibilities are outlined in the following section.

It is important to stress that this is an engineering organization, and the skills and background of the staff are significantly different than those of existing operational security departments. The staff of most existing security departments have military or law enforcement backgrounds, and are oriented towards enforcement and physical/personnel security policy, not engineering software/systems security solutions.

2.3 Roles and Responsibilities

Due to the recommended distributed responsibility for the implementation of security engineering, many parts of the ITS engineering organization will have roles and responsibilities in this area. Listed below are suggested starting points for defining organizational responsibilities in the security engineering domain.

2.3.1 Security Engineering

The FDOT central security engineering organization shall have the following roles and responsibilities:

- Create and maintain all security engineering-related processes, policies, and operating procedures at the ITS organizational level.
- Participate in project design reviews and provide approval for security-related aspects of project requirements, design, implementation, and testing.
- Provide technical assistance to projects in the area of security engineering.
- Provide regulatory guidance for security-related requirements in conjunction with the FDOT Legal Office.
- Obtain and maintain any regulatory mandated certifications for security engineering.

- Maintain a liaison with FDOT operational security staff for deployed projects to incorporate field data about actual and emergency threats into policy and practice throughout ITS.

- Support the creation and maintenance of security engineering training.

- Liaison with law enforcement agencies and industry groups to maintain a knowledge base of present and emerging threats against IT and transportation assets.

2.3.2 Systems Engineering

Systems engineering personnel for ITS projects shall have the following roles and responsibilities:

- Perform threat analysis with support, as required, from security engineering.

- Perform vulnerability analysis with support, as needed, from security engineering and software engineering.

- Ensure that security engineering requirements and processes are flowed down to project subcontractors.

- Manage risk analysis to determine the vulnerabilities to be addressed.

- Prepare the test plan, and manage test execution of security evaluation and/or accreditation testing.

2.3.3 Software Engineering

Software engineering personnel on ITS projects shall have the following roles and responsibilities:

- Design and implement countermeasures in accordance with security engineering guidelines and/or policies.

- Review software during design and development phases to identify additional vulnerabilities.

2.4 Security Engineering Management

Much like any systems engineering activity, the security engineering process will be managed by engineering reviews, audits against applicable policies/standards, and measurement via appropriate metrics.

2.4.1 Reviews

In the spirit of integrating security engineering practice across the engineering disciplines, all project design reviews shall address security engineering aspects. It is suggested that checklists be prepared by the security engineering staff for inclusion in design review procedures to assist other engineering disciplines in properly addressing the security domain in their reviews. It is also suggested that security engineering staff attend preliminary design reviews (PDRs) and critical design reviews (CDRs) to assess system security maturity.

If formal security evaluation/accreditation is required, the FDOT shall conduct a formal test readiness review (TRR) chaired by security engineering staff to ensure successful evaluation. This is good practice since formal evaluations and accreditation testing is usually performed or witnessed by certified third parties, and encountering test problems or failures will impact project cost and schedule.

2.4.2 Governance

It is recommended that the FDOT work towards developing policy and guidelines to provide governance over the execution of security engineering activities. While security engineering plans based on this document are a primary form of governance, it is also good practice to develop additional technical guidelines/policies to ensure uniform compliance with proven best practices as well as flow-down of applicable regulatory requirements.

2.4.3 Metrics – *To Be Determined*

3. Security Engineering Activities

3.1 Security Engineering Process

3.1.1 Standard Practices

The FDOT shall develop a security engineering practices manual (SEPM) to provide guidance to project engineers when performing standard security engineering activities. Project engineering staff shall conduct their security engineering efforts in accordance with this manual except where tailored by the project security engineering plan. In addition, project activities shall comply with any security engineering policies or other security engineering governance as discussed in S*ection 2.4.2* of this appendix.

3.1.2 Project-Specific Processes

An FDOT project may tailor the security engineering process via the project security engineering plan. For instance, the verification process will often be tailored based on whether the project has external interfaces that are required to conform to formal security policy or regulations. Security verification to industry/federal standards can be quite costly, and will usually be conducted only when required for interoperability with external systems or the public. Practices dealing with Internet connectivity may also be tailored in cases where the project system does not directly connect to public networks.

A specialized type of project that will require a tailored process is retrofitting an existing system to provide security services. While the fundamental threat, vulnerability, and countermeasure process should be followed, many of the practices likely to be included in the SEPM will assume original design, not modification or "bolt-on" security services. In this case, the project will need to tailor these processes using the security engineering plan.

3.2 Threat Analysis

Threat analysis is one of the three fundamental security engineering activities. Comprehensive identification and accurate assessment of threats to a system is critical to developing a cost-effective security policy. Without an accurate threat model, systems can be either overprotected, designing countermeasures for potential vulnerabilities with no realistic threat to produce them, or underprotected, overlooking vulnerabilities without a threat model to drive an analysis. Two threat model aspects will be discussed – identification of threats and assessing the capability/probability of the threats.

3.2.1 Identification

Threats must first be identified before meaningful security engineering can be conducted. Personnel performing threat identification shall consider potential threats to the system in the following categories:

- **Human Threat –** This is a deliberate or accidental act by any person, authorized or not. It will be useful to further categorize these threats as internal and external to the FDOT. Examples may include user errors, unauthorized access attempts, and data sabotage.

- **Technical Threats –** This is a malicious or accidental attack by software or a network. Common examples include viruses, worms, Trojans, and network level denial-of-service (DOS) attacks.

- **Physical Threats** – This is the malicious or accidental damage to a system through physical acts. Examples may include hardware sabotage or failure. These types of threats primarily impact system availability, as opposed to privacy or confidentiality. This category also normally includes acts of war or civil disturbance.

- **Natural/Environmental Threats –** These are natural or manmade events that damage or impair a system. Common examples include fire, flood, storms (including lightning), and earthquakes.

Sources of threat identification include:

- **Law Enforcement** – The FDOT security engineering team should establish working relationships with federal, state, and local law enforcement agencies to obtain general and specific threat information.

- **Professional Organizations –** Computer security organizations such as SANS and CERT maintain extensive databases of threats and vulnerabilities, and countermeasures.

- **Operations History –** Operational histories are valuable sources of threat information in the analysis of incidents in existing systems.

- **Consultants**

- **Design Engineers** – The same engineers that design the system are often quite inventive on how to attack it.

- **Hacker Web Sites/Publications –** Spying on potential attackers is effective, but time consuming (the signal-to-noise ratio is quite poor).

3.2.2 Capabilities

Once threats are identified, project personnel shall assess the expected capability of the threats. Capability can refer to skill in the case of human threats, sophistication of technical threats, and severity of natural threats.

In addition to estimating the capability of a threat, personnel shall also attempt to assess the probability of the threat occurring. Important factors to consider are the possible motivation of the attacker and the perceived value of the target system. For example, it is highly unlikely that an attacker would launch a highly sophisticated technical attack requiring national technical assets against a target system with no substantial financial or national security value.

3.2.3 Threat Database

It is recommended that the security engineering organization maintain an online database of threats. This database will be a valuable resource for projects to use in creating system-specific threat models.

3.3 Vulnerability Assessment

Vulnerability analysis is the second of three fundamental security engineering activities. This activity identifies the consequences to the system from a specific threat, should that threat occur, and predicts the impact to FDOT services and the liability of that vulnerability.

3.3.1 Identification

Once threats are identified via threat analysis, system vulnerabilities to those threats must be determined. These vulnerabilities are often comprised of a first and second order effect. The first order effect is the immediate result of a successful attack (i.e., the attacker gaining access to a valid user account via the threat of password guessing). The secondary effect is the consequence to the system function or users (i.e., the compromised user's information being altered or stolen).

It is recommended that the project create and maintain a traceability matrix that correlates a system vulnerability to specific system components (e.g., a software module). Using this matrix, engineering can easily identify which vulnerabilities need to be reassessed as software or hardware is redesigned or modified.

3.3.2 Impact Assessment

The project shall prepare an assessment of the impact to the system mission and/or the business operations that rely on the system. These impact assessments shall include, at a minimum, interruptions to mission critical services provided by ITS, potential civil liabilities incurred as a result of the vulnerabilities, regulatory/statutory failures, and the impact to operating budgets. Engineering will need to involve other FDOT organizations, such as the Legal Office and the Financial Planning Office, to perform a comprehensive impact assessment.

3.3.3 Risk Analysis

The final stage of vulnerability assessment shall weight the vulnerabilities identified based on the threat probability and impact assessment. The goal is to provide a means to prioritize how vulnerabilities will be addressed. Obviously, vulnerabilities that are the result of high probability threats and have significant impacts to ITS operation and public safety should be weighted more heavily.

Once the vulnerabilities are weighted or ranked, project engineering should incorporate system requirements that reflect the threats and vulnerabilities that present significant risks to the system and the FDOT ITS Program.

3.4 Countermeasure Design

The final basic activity is the design of the countermeasures needed to address the vulnerabilities and threats identified previously.

3.4.1 Security Architecture

Successfully integrating security engineering into an ITS project usually requires the adoption of a security architecture. A security architecture provides structure and cohesiveness to a security design, in the same manner that software and hardware architectures are necessary to organize the design and implementation of the respective engineering solutions.

Security architectures are typically constructed around a security policy. Policies are often derived from an underlying formal security model, such as the Bell-LaPadula model for multilevel security,[82] although many policies are expressions of security strategy based on empirical data (i.e., best practices information) rather than a rigid mathematical model. Whatever the genesis, security policies are necessary to provide guidance to the security engineer(s) developing the security design.

[82] Bell, D.E. and L.J. LaPadula, *Secure Computer System: Unified Exposition and Multics Interpretation* (1974). Contract No. F19628-75-C-0001, Report No. ESD-TR-75-306.

Intelligent transportation system projects shall document the security policies to be used on that project. It is recommended that projects also create and document a security architecture around the policies. The architecture should define and describe the technologies, operating principles and broad software/hardware structure of the security solution.

3.4.2 Candidate Trade Studies

Once an architecture is defined, ITS projects shall identify candidate solutions to address specific vulnerabilities. These candidates shall conform to the security policies and architecture. This phase of the security engineering process is similar to any other engineering design trade study.

It is important to consider not only the capability of a candidate countermeasure to address the vulnerability, but any side effects on system operation as a result of the security design. It is quite easy to adopt invasive countermeasures that effectively address vulnerabilities, but also unacceptably impact normal system operation. Security engineering is, like any other engineering discipline, a compromise between technical function, affordability and mission.

Intelligent transportation system projects should incorporate the selected countermeasure designs into software and hardware requirements where applicable.

3.5 Security Verification and Testing

As in any other engineering discipline, comprehensive and accurate testing of a design is necessary to ensure that it is robust. Verification and testing of a security design is typically separated into two activity types referred to as assurance and evaluation. Assurance is the process of determining whether the system will function as designed; evaluation is the process of proving it to others.

3.5.1 Assurance

Security assurance is a process consisting of the traditional engineering techniques of analysis, inspection, and testing towards the end of verifying that a specific ITS project is secure. By integrating security requirements into the system, and component requirements and specifications as recommended throughout this plan, the FDOT will cover testing of security functionality by the performance of the normal system and unit tests per the usual RVTM.

3.5.2 Formal Evaluation [Optional]

Evaluation is the formal process of demonstrating achievement of the assurance target. Security evaluation can take two forms – evaluation by the relying party and evaluation by third parties. Relying party evaluation relies on the relying (or using) party to define and accept the results of the testing program. In the case of ITS, the replying party would normally be the FDOT. The organization responsible for conducting and reviewing the testing would be the FDOT's ITS security engineering organization. In cases where part, or all, of the security requirements are dictated by other state or federal agencies, or by regulatory fiat, the relying organization may be the agency that created the requirements or that is charged with administering the regulations. This form of evaluation will be planned and conducted similarly to system-level acceptance testing.

Third party evaluations are performed by third party organizations with no financial or operational interest in the outcome of the evaluation testing. These evaluations can also involve certification, also referred to as accreditation, by the third party to previously established standards or processes. This aspect of evaluation is addressed in the following section.

It is recommended that the FDOT mandate formal security evaluation for any future ITS project possessing the following characteristics:

- Projects that provide direct public electronic access, either via the Internet or by dedicated devices/protocols (e.g., ***SunPass***)

- Projects that connect to other ITS or state/federal systems via public infrastructure (e.g., the Internet or wireless communication)

- Projects that connect to external systems that, in turn, offer public access

Furthermore, the FDOT should work towards mandating formal evaluation for any ITS product or project that is interconnected with other internal (i.e., the FDOT ITS services) or external (i.e., state/federal/commercial) information systems or devices.

3.5.3 Security Certification [Optional]

Certification or accreditation is evaluation to a standard or process that can be used as demonstrative proof of achieving a predefined security assurance level. Presently, the Common Criteria program is the evolving international security evaluation standard. In the United States, the Common Criteria is promoted and controlled by the National Information Assurance Partnership (NIAP), a collaboration between the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST). Secondary certification standards that may be applicable to the FDOT include the Federal Information Processing Standard (FIPS)[83] and the Program Review for Information Security Management Assistance (PRISMA).[84] Both of these efforts are overseen by NIST as well.

While the FDOT should begin the process of familiarization with these certification standards for future interoperability, there is little to be gained from formal certification until mandated by regulation/statue or required by external systems.

3.6 Incident Reporting and Investigation

As mentioned earlier, the FDOT's ITS security engineering team shall create and maintain a database of threats and vulnerabilities to aid in the analysis and design of security solutions for future systems as well as ongoing improvements in existing systems. The security engineering organization shall participate in the technical investigation of security incidents on deployed systems, and propose improvements to existing infrastructure based on lessons learned from current operations.

4. Security Training

Security awareness by both engineering and operations staff is a significant component of the FDOT's ITS security plan. Many serious threats and vulnerabilities can be recognized and thwarted during the design of an ITS product if all engineering disciplines are aware of basic security principles, and common threats and vulnerabilities. Likewise, security policy and operating procedures are more likely to be followed if operations personnel understand the ramifications of security breaches and lax enforcement of policy. To this end, the FDOT ITS Section shall develop and administer security awareness training to all ITS engineering and operations staff. The security engineering organization shall take the lead in developing the course material based on emerging threats and lessons learned from previous projects.

Intelligent transportation systems engineering shall also develop or obtain technical security engineering training for selected engineering personnel in order to provide internal security engineering expertise.

[83] More information regarding the FIPS publications is available online at http://www.itl.nist.gov/fipspubs.

[84] More information regarding PRISMA is available online at http://prisma.nist.gov/.

This page is intentionally left blank.