Cybersecurity and Intelligent Transportation Systems

A Best Practice Guide

www.its.dot.gov/index.htm

Best Practice Guide – September 17, 2019
Publication Number: FHWA-JPO-19-763

U.S. Department of Transportation

Produced by Noblis. Inc.
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
ITS Joint Program Office

Notice

Technical Report Documentation Page

1. Report No. **FHWA-JPO-19-763**	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle Cybersecurity and Intelligent Transportation Systems: Best Practice Guide		**5. Report Date** September 17th, 2019 **6. Performing Organization Code**
7. Author(s) Cory Krause, Justin Anderson, Kellen Shain, Linda Nana, Tom Mazzone, Stephen McNaught, Mark Jackson		**8. Performing Organization Report No.**
9. Performing Organization Name and Address Noblis, Inc. 500 L'Enfant Plaza, S.W. Suite 900 Washington, D.C. 20024		**10. Work Unit No. (TRAIS)** **11. Contract or Grant No.** DTFH6116D00036L
12. Sponsoring Agency Name and Address ITS-Joint Program Office 1200 New Jersey Avenue, S.E. Washington, DC 20590		**13. Type of Report and Period Covered** Final Report, Sept 19, 2018 – Sept 18, 2019 **14. Sponsoring Agency Code** HOIT-1
15. Supplementary Notes Work performed for: Kate Hartman, ITS JPO		
16. Abstract This report presents the best practices in Intelligent Transportation Systems Cybersecurity, particularly in the planning and conducting a Penetration Test. The report details the methodology of scoping a test; including the objectives, requirements, success criteria, test type, management, and test readiness. The report is completed with a template test plan to start local and state DoT's in their own cyber security plan and penetration test.		
17. Keywords Penetration Test, Intelligent Transportation Systems, Cybersecurity	**18. Distribution Statement**	
19. Security Classif. (of this report) unclassified	**20. Security Classif. (of this page)** unclassified	**21. No. of Pages** 74 / **22. Price**

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Table of Contents

List of Figures

List of Tables

1 Introduction

A Department of Transportation (DOT) agency will require decisions on several topics when conducting effective Penetration Testing (PT) of the Intelligent Transportation System (ITS) for the managed locality. The ITS PT provides evidence of exploitable vulnerabilities in the ITS operations, management and governing policies for cybersecurity protections of the ITS. The PT can illustrate both actual and potential impacts resulting from test attacks, thereby providing insights into the risk to locality transportation for the people, businesses, organization and broader population relying on safe ground transportation in and through the locality.

An ITS consists of information and communication technologies applied to transport infrastructure such as road networks, traffic and transit systems with objectives to: reduce traffic congestion and the environmental impacts; enable vehicle operators to make informed decisions; improve safety and transport efficiency; support connected vehicle initiatives to increase communications and take advantage of new applications using increasing computing in vehicles. As a result, traffic signal systems and traffic management systems use increasing Information Technology (IT) relative to the Operational Technology (OT) in these systems. Protecting the mix of technology and systems in ITS requires a wide range of technical and operations solutions.

Recent security incidents involving adversaries using "ransomware", malicious software designed to encrypt information on the target systems and demand a ransom to obtain the decryption key and recover the data, have been directed at locality government services at city and smaller community levels [1] . In the case of an attack in San Francisco, the target was the Municipal Transportation Agency and toll collection services. Attacks are being directed at United States electric grids and other critical infrastructures will be in the adversary radar are candidates for attack today [2] .

ITS Cybersecurity in Context

ITS are combinations of IT and OT and require complex cybersecurity protections. NIST Critical Infrastructure Cybersecurity Framework and the DHS Implementation Guidance for Transportation provide context for using Penetration Testing as a mechanism to identify vulnerabilities and impacts driving risk with a DOT ITS deployment. The DOT should move beyond a reactive mode for responding to penetration test results in order to achieve effective DOT risk reduction.

A DOT for every region in terms of area and population relying on ground transportation must put in place cybersecurity management programs to address potential risks with increasingly connected and automated transportation systems using ITS and supporting technology. Previous generation systems utilizing less automation and requiring manual operations leave DOTs with the challenge of predicting the impacts of new service and technology introduction on secure operation and safety. The DOT staff with years of experience with legacy systems may share some fallacies observed with other utility services providers and OT experience:

- Vendors configure their equipment with secure default configurations.
- Secure configuration specifications can be located when needed.

- The critical operations networks are air-gapped, meaning no means of external electronic connection.
- Radios with proprietary protocols and modulation schemes are extremely difficult to attack.
- Although we are a government agency, our security approach and implementation are not public.
- Most adversaries and the sophisticated threat sources would pick higher profile targets.

These assumptions are wrong and lead to vulnerable ITS designs and implementations.

Penetration Testing is one of the Center for Information Security (CIS) Top 20 Critical Security Controls for Effective Cyber Defense[1] and is included within the broader set of program security activities from the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* [3] . The Cybersecurity Framework (CSF), created through collaboration between government and the private sector, uses common language and provides mechanisms to establish a new cybersecurity program and strengthen existing programs to reach repeatable and adaptable implementations. The CSF mechanisms support an organization such as a DOT to:

- Describe their current cybersecurity posture/state
- Describe their target state for cybersecurity
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- Assess progress toward the target state
- Communicate among internal and external stakeholders about cybersecurity risk

The U.S. Department of Homeland Security *Transportation Systems Sector Cybersecurity Framework Implementation Guidance* provides guidelines for applying the framework to transportation systems [4] . The guidance describes how to apply the tenets of the NIST CSF to reduce cyber risks of critical transportation infrastructure such as an ITS.

Applying the framework begins with establishing a DOT cyber-risk profile. A risk profile attempts to determine the DOT's willingness to take risk (or its aversion to risk), which drives the overall decision-making strategy. The risk profile is established after examining internal and external factors. From the *Guidance*

> "*Assessing the internal context of the organization will show what countermeasures are in place while providing an overall snapshot of how the organization views its cybersecurity program. That combined with the external context, consisting mainly of threat intelligence provided by the Department of Homeland Security and other intelligence/threat resources [and external partners and supporting agencies], will help the organization align capabilities deployed to [mitigate] external threats*." (p. 6)

The Framework Core focuses on five key functions needed to drive a comprehensive cybersecurity program:

[1] Information available at the Center for Internet Security site https://www.cisecurity.org/critical-controls/

- **Identify** risks to resources supporting critical functions
- **Protect** these resources and limit the impact of cybersecurity events
- **Detect** incidents that have occurred
- **Respond** to the detection of events
- **Recover** following response procedures

Penetration testing provides indications of the feasibility of attacks exploiting the target DOT ITS vulnerabilities and the effectiveness of current security protections for the ITS infrastructure (**Protect** and **Detect**). In addition to using penetration testing as a source of information for ITS vulnerability analysis, penetration test results provide indications of threat likelihood, specifically opportunity to attack and likely succeed. Finally, a penetration test indicates directly, or by estimation, the potential impact on the ITS. These factors combine to rate relative risk during risk analysis (**Identify**). Thus, a DOT performing ITS PT is performing an activity contributing to the larger DOT cybersecurity and safety risk management program.

Use Penetration Testing in ITS Security Management

- Start with a broad assessment of ITS security management.
- Focus on critical functions and supporting subsystems but cover all.
- Require PT for all projects adding new technology and infrastructure.

An ITS PT will be most effective when executed as a repeated activity of the DOT security management program within which ongoing assessment and corrections are managed. A DOT security program structure and implementation can be characterized along a qualitative scale such as the risk management Implementation Tiers of the NIST CSF or the cybersecurity program maturity levels in the Cybersecurity Capability Maturity Model (C2M2) defined by the Department of Energy and Department of Homeland Security [5] . In terms of approach to cybersecurity practices, the levels can be summarized as:

- *Reactive* to events with ad-hoc pulling of resources, to **Respond** and **Recover** from damaging events
- *Compliant* with standards and guidelines for security controls
- *Proactive* using continuous monitoring and planning mitigations for effective resolution, to minimize organization and public risk.

The ITS Penetration Test will most effectively guide risk reduction when the DOT security program has identified the ITS risks. Mitigation of uncovered vulnerabilities to the ITS deployment and operation can be prioritized based on reduction of the risks. The ITS PT may identify more previously unknown vulnerabilities, uncovered by successful attack scenarios with potential significant impacts, requiring more mitigations than the DOT has the resources to address. Without the understood DOT program risk profile, prioritizing the mitigation efforts will require establishing a new consensus on the DOT risk reduction priorities for the ITS in a *Reactive* mode, a sometimes contentious, time consuming process without necessary resources planned and budgeted by the DOT.

The goal of the ITS PT is to identify vulnerabilities in the locality of DOT ITS infrastructure through targeted attacks aiming to cause or demonstrate undesirable outcomes. The penetration testing concepts for DOT ITS are summarized in [6] .   A well-planned PT does not require the causing of significant disruptions in order to demonstrate attack proofs of concept. Penetration testing is used to uncover vulnerabilities and risks with ITS OT (sensors, cameras, traffic lights, control systems) where impacts to control system operation can include physical and human damages. As described in the following sections, the PT test team and stakeholders can plan ITS PT to minimize disruption of ongoing ITS operation and maintain ground transportation safety.

An important PT outcome for the DOT is receiving recommended mitigation actions from experienced penetration testers. Some mitigations may be directed at technology implementation, configuration and system activity monitoring. In some cases, recommendations will address the ongoing activities of the DOT cybersecurity program and administrative operations. Thus selecting the penetration testers from an experienced organization with knowledge of ITS environments, technology, industry standards, operations and using appropriate testing methods discussed in Section 5 will provide the best view of cybersecurity risks with the target ITS operation.

1.1 Document Organization

The remainder of the document is organized as follows:

- Section 2 provides recommendations for the PT management, establishing test requirements and criteria for success.
- Section 3 provides recommendations for selecting what to include within the scope of the ITS PT.
- Section 4 discusses recommended topics to document in the ITS PT Plan and communicating with stakeholders, including considering the maturity of the DOT security management program.
- Section 5 describes recommended controls for the PT execution and tradeoffs about results.
- Section 6 discusses options and a basis for selecting whom to perform the ITS PT.
- Section 7 describes recommended content to request in the ITS PT Report.
- Section 8 discusses appropriate next steps, both for correcting flaws identified by the PT, determining risk impacts, and shaping the DOT security management ongoing assessments.
- Section 9 contains a list of document references.

1.2 Acronyms

The following acronyms are used in the document.

ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
ATC	Advanced Transportation Controller
CCTV	Closed Circuit Television, Camera
CERT	Computer Emergency Response Team
/CC	CERT Coordination Center
CIS	Center for Information Security
CREST	Council of Registered Security Testers
CSF	NIST Cybersecurity Framework
CV RSE	Connected Vehicle Roadside Equipment

CVSS	Common Vulnerability Scoring System
DMS	Dynamic Message Signs
DoS	Denial of Service
DOT	Department of Transportation
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISECOM	Institute for Security and Open Methodology
IT	Information Technology
ITS	Intelligent Transportation System
JTAG	Joint Test Action Group
MMU	Malfunction Management Unit
MNDA	Mutual Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency/Internal Report
NVD	National Vulnerability Database
OS	Operating System
OT	Operational Technology
OWASP	Open Web Application Security Project
POC	Points of Contact
PT	Penetration Test
PTES	Penetration Test Execution Standard
RF	Radio Frequency
RSU	Road Side Unit
SME	Subject Matter Experts
SMS	Short Message Service
TMC	Traffic Management Center
TRR	Test Readiness Review
USB	Universal Serial Bus
USDOT	United States Department of Transportation

2 ITS Penetration Test Planning

A consistent recommendation from PT methodologies in a number of standards and guidelines is creating a plan to describe and communicate the goal and objectives of the test, requirements for execution of testing, the infrastructure coverage of the test, management Points of Contact (POC), schedule and the basis for categorizing the PT as successful for the DOT.

Several Penetration Testing guidance references provide a good understanding how a PT can be managed and safely conducted as background for the DOT ITS PT stakeholders and managers.

- The Council of Registered Security Testers (CREST) is a non-profit accreditation organization with guidance on running an organization penetration testing program [7] .
- The PTES Team provides comprehensive guidance on conducting a PT in the Penetration Test Execution Standard with a compendium of tools and attack techniques described in the Technical Guidelines [8] [9] .
- Penetration testing guidelines for software and applications used with ITS system management are available from the Institute for Security and Open Methodology (ISECOM) and the Open Web Application Security Project (OWASP) [10] [11] .

PT References and Stakeholder Concurrence with the Plan

Many independent guidelines are available to guide ITS penetration testing. Establish the DOT stakeholder POCs with goal of putting in place the remediation plan for uncovered weaknesses leading to significant transportation impacts.

The PT Plan topics and management structure are discussed in the following sections. A template PT Plan document is included in the Appendix. The template provides a starting point for structuring a DOT ITS PT engagement and communicating the plan to stakeholders.

The ITS PT Plan should be baselined with concurrence of the DOT and Penetration Tester organization authoritative representatives. Although not intended to be a legal document, requiring review by participant legal representatives as would a contract Statement of Work, the document is a valuable reference for all participants during testing through reporting of results. The following sections discuss some approaches and options for ITS PT planning.

2.1 Test Objectives

In general, the objective of an ITS PT is to identify the exploitable vulnerabilities in the DOT ITS environment, categorize the severity of the vulnerabilities exploited through successful attacks, and receive experienced recommendations for mitigating risks to public transportation from ITS operation. Depending on the cybersecurity maturity of the DOT and available prior PT results, a PT objective may be more focused on impacts of recent changes to the ITS management, operations and administration, or technology. When a PT is performed on the DOT ITS for the first time, the test objective may be establishing indications of all types of security control gaps existing in the current ITS implementation and operations. For an initial ITS PT, the goal should include discovering design, operations, administration and technical security control gaps with enough “proof of concept” to assess the impacts from successful attacks exploiting the existing vulnerabilities. The relative impacts provide a basis to prioritize remediation actions.

The ITS PT objectives can frame the scope of the PT activity, discussed in more detail in Section 3.1. The DOT objective can be very focused or broad, such as identifying security weakness through demonstrated exploitable vulnerabilities. The PT uses attacks directed at discovered weaknesses so the DOT PT objectives should be framed by a view of threats to the locality transportation infrastructure. Some examples of potential vulnerability sources to examine include:

> **Establish the PT Objectives**
>
> ITS PT objectives can be broad – extent of exploitable vulnerabilities impacting local transportation – to focus on new systems and functionality introduced in the ITS infrastructure – to Operations changes targeting efficiency. State the objectives to drive effective PT planning.

- Replacement of a vendor Traffic Signal Controller with an enhancement or different vendor product
- Introduction of new video surveillance supporting law enforcement
- ITS vulnerabilities with significant impact to ground transportation in a sensitive area
- DOT ITS security operations ability to detect unauthorized activity and recover prior to disruption of traffic
- The technology and configuration supporting the critical ITS functions
- New interfaces, protocols and procedures used to communicate with a regional ITS.

Management of risk mitigations for discovered vulnerabilities and ITS impacts occurs after the PT. The DOT risk management processes will consider the attack likelihoods and demonstrated or projected impacts to locality transportation, as rated by penetration testers, and compare ratings to the DOT risk profile. Thus, an important output from the ITS PT are the ratings of vulnerability severity and exploit impact combined with recommendations for remediation by Penetration Test Subject Matter Experts (SME). The testers executing the attacks know the controls that would have prevented or diverted the attack executions. Improving the risk profile of DOT ITS operations can be based on the recommendations and provide the basis for requesting internal DOT resources to complete priority remediation activity.

2.2 Test Requirements

Testing for systems, applications, components, sensors and operations processes should occur throughout the development lifecycle and initial deployment. The testing is driven by specific requirements documented and approved in test plans. For example, compliance testing will include test cases to verify all applicable requirements in the applicable standards are met by the system configuration and operation. At this point in time, independent security compliance test results are not available for most ITS components. Thus, the cyber security vulnerabilities in an ITS configuration are difficult to identify from the combination of individual components.

Penetration test requirements can be written to identify the specific systems and components of the ITS to be tested including applications, network segments, and external interfaces relative to the ITS infrastructure. PT requirements should address protection of confidential or sensitive information during and after completion of the penetration test engagement.

If specific types of tests are required, such as new device firmware examination and protections applied during vendor update procedures, requirements should be written identifying the target devices and capabilities. Test requirements agreed to be met by the penetration test organization provide a means to verify test results will reflect the target ITS scope, described in more detail in Section 3.

Document PT Requirements

Document penetration test requirements for specific ITS systems and operations targets. Only include types or nature of attacks when examining effectiveness of mitigations for problems uncovered in a previous PT.

Penetration testing involves some reconnaissance and examination of potential weaknesses in the target systems and operations. Attacks on potential weaknesses are chosen or adjusted based on the preparation activity. Thus, test requirements should not attempt to define actual attacks or attack sequences unless the PT objective is to examine the effectiveness of new mitigations for vulnerabilities demonstrated from prior PT successful attacks.

The DOT has options for documenting, reviewing and obtaining management approval of the PT tests. If the ITS target of the PT is limited and the number of requirements relatively few, the requirements can be included within the PT Plan document discussed in Section 4. When the PT scope includes many functional components of the ITS, multiple external interfaces, and many types of penetration tests, the DOT should document the requirements separately for review by technical experts and management. The PT Plan can reference the requirements and be approved by management separately.

2.3 Criteria for Success

The DOT should determine the success criteria for the PT so the Penetration Testers and DOT management shape and bound the test execution and resources applied to produce results meeting the criteria for success. The criteria can be general

- The approved PT Plan was executed within schedule and delivered recommended ITS mitigations to reduce risk of demonstrated attacks and transportation impacts.

Or focused on a particular area

- The ITS Wide Area Alert system protections prevented malicious disabling of alert information distribution or modification of information between the Emergency Management Center and the supported traveler information sources.

Or the DOT could have programmatic criteria

Determine Criteria for PT Success

Effective planning of an ITS PT requires determining the organization criteria for success. Counts of vulnerabilities discovered or successful attacks are not useful criteria driving effective remediation and improved critical infrastructure security. Consider measurable cybersecurity improvement in security control implementation and risk reductions.

- The PT of the new Traffic Management System did not demonstrate critical vulnerabilities requiring changes or enhancements prior to deployment or full operation.
- The PT demonstrated the need to establish a DOT risk profile to guide management of ITS changes to reduce risks uncovered in the PT.

The ITS success criteria should not be based on number of successful attacks, extent of impacts uncovered, or other metrics that can be manipulated through the resources applied to the testing. The resources are specified in the PT Plan as described in Section 4. All the ITS PT stakeholders should know the success criteria and perform the planning and execution to meet the success objectives. Communicating the objectives and success criteria can be done in the ITS Penetration Test Plan document.

A successful ITS PT requires determining a realistic scope for the testing. Complete testing for a metropolitan ITS will take time and resources from the DOT to manage execution, especially targeting the live deployed ITS, as well as diverse technical expertise of the penetration testers. The next sections describe considerations for the DOT in defining PT purpose, scope and managing ITS coverage for an initial engagement. The ITS PT Plan and a document template are described in Section 4.

3 Penetration Test Scope

The scope of the ITS penetration test can include security policies, devices, applications, networks, access controls, communications and configurations that comprise the locality ITS infrastructure as well as interfaces to external systems or Regional ITS managed by other entities. A relatively small ITS in a small city may lend itself to a single PT project without hindering normal DOT ITS management and operations. Usually available resources and time put limitations on the scope of a PT. Over time, a DOT should examine all the critical functions of supporting systems of their ITS.

Penetration test execution can be a slow process requiring manual testing adjustments based on the results of test activity and capturing result evidence, so effective penetration testing requires time and knowledgeable personnel to devise penetration attack methods, sequences and resources to address the range of components deployed in a large ITS. The staff available to manage, monitor and respond during PT activity is expected to limit the scope of the ITS PT.

The potential domains of a DOT ITS considered for a penetration test include

- Organization, including business functions and people managing and operating the systems
- Physical infrastructure including the ITS components and field locations
- Business infrastructure including IT and Business applications and interconnects to other agencies or third parties
- Wired and Wireless network segments within the ITS infrastructure and external network connections
- Cloud hosted services and infrastructure including Operations and Supporting services
- Resources used by contractors providing support for the ITS.

The ITS PT objective may set the scope of the PT. When the objective is broad, we recommend focusing the penetration test on the most critical functions and the implementation in the ITS. Critical ITS functions and supporting components can be determined through applying the NISTIR 8179 *Criticality Analysis Process Model: Prioritizing Systems and Components* [12] . The analysis can consider operational, environmental and safety consequence categories for system or component failures.

Address the Critical ITS Functions

The DOT organization responsible for the ITS needs to determine the critical functions to target with Penetration Tests. Over time, look for exploitable vulnerabilities across the entire ITS infrastructure.

The United States Department of Transportation (USDOT) National ITS Reference Architecture defines common ITS subsystems – Center, Support, Field, Traveler, and Vehicle - described in the next section. An initial ITS PT should examine the implemented Center, Support, Field subsystems and the network communications between all the ITS subsystems.

If the DOT uses a public cloud service, the contract arrangement may not permit active penetration testing of the cloud provider infrastructure. However, ITS PT should include attack scenarios in the penetration test through any hosted services and providers for critical functions. Concurrence with the cloud provider on rules of engagement is recommended (see Section 6).

Within the subsystems of an ITS are many functions with supporting systems and devices. In the next section, we discuss considerations and choices available for including functional subsystems and components in the ITS PT. Note a PT can be used to test operations effectiveness, such as incident response and recovery, since test attacks can trigger incidents and response effectiveness observed and measured by the DOT.

3.1 Infrastructure in Scope

The Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT)[2] provides a common model for considering where penetration testing can be applied to a DOT ITS infrastructure. Figure 1 depicts the physical and functional subsystems of an ITS. A DOT ITS deployment may include a subset of these subsystems.

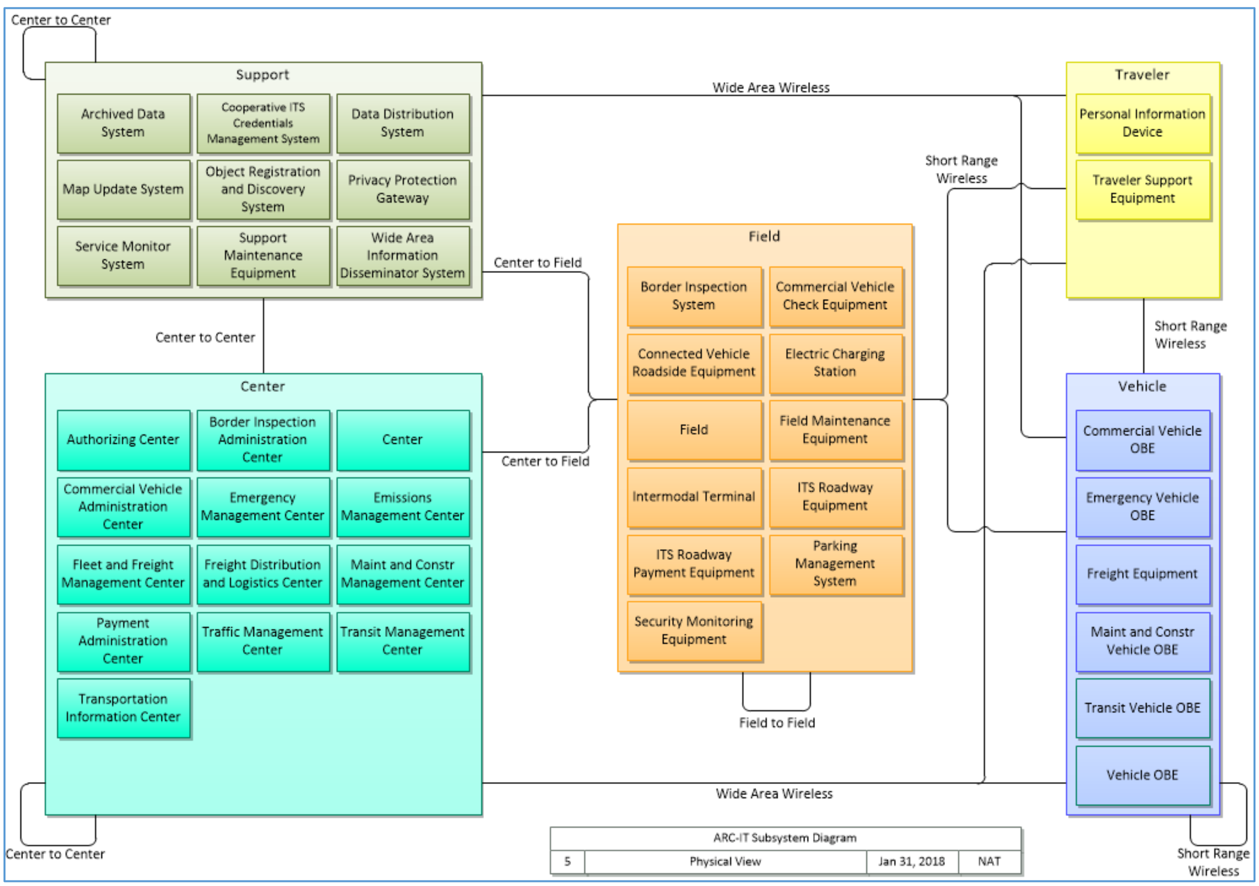

Figure 1 ARC-IT ITS Architecture (Source: USDOT)

[2] ARC-IT and the accompanying toolsets help implementers develop regional architectures to effectively meet their needs and ensure regulatory compliance, while facilitating efficient, secure, and interoperable ITS deployments. ARC-IT and its accompanying software tools are available at no cost from www.arc-it.net.

Completing a Criticality Analysis will provide a view of which ITS functions, processes and supporting systems in the architecture are more critical to the local transportation operations. Systems that are more critical should have a higher priority for inclusion in PT scope.

Example of critical operations to include in the ITS penetration testing program are:

- Center – Transportation centers are a combination of personnel and systems that monitor and manage the Intelligent Transportation System from a fixed location away from field devices and roadway networks. It also consists of the networking that supports ITS systems. Critical components of the center include the personnel, networking, server systems, and web applications associated with Center-to-Field and Center-to-Center interactions.
- Support – The support center consists of operations and systems that serve non-transportation purposes, such as communications, security, or management. Critical components of Support center include the server systems and web applications associated with Center-to-Field and Center-to-Center interactions.

Start with Criticality Analysis, Center and Field Subsystems

Initial Penetration Tests need to focus on Center, Field and Communications subsystem and critical ITS functions identified from a Criticality Analysis.

- Field – The field consists of devices in proximity to the road network that function as surveillance (e.g. traffic sensors, Closed Circuit Television (CCTV) cameras), traffic control (e.g. traffic signal controllers), public messaging (e.g. Dynamic Message Signs (DMS)), and toll collection (e.g. parkway tolls, parking). Critical components of the Field include traffic signaling, the public messaging system, the surveillance system and the wireless and wired networks that support them.
- Traveler – The traveler field consists of equipment used by a person traveling the public roadways to access public transportation services (e.g. emergency notifications, real-time public transit schedules). Ensuring that the traveler is notified with emergency and non-emergency data so that they can respond appropriately is critical.
- Vehicle – This includes commercial and non-commercial vehicles of various sizes, and cargo, as well as the on-board electronic systems such as navigation. Critical components related to the Vehicle area include onboard devices that generate and receive data with ITS services.

In addition to the previous five areas, the communications between them are critical beyond the coverage as part of Support.

- Communications – The communication components of the ITS consist of very diverse wired and wireless technologies that may include WiFi[3], WiMAX[4], MDS™ [5] and cellular networking. They

[3] WiFi is a trademark of the WiFi Alliance which means IEEE 802.11x
[4] WiMAX is a trademark and service mark of the WiMAX Forum
[5] MDS™ is a Trademark of General Electric Company

can utilize encrypted or non-encrypted access controls and protocols. As technology advances, field maintenance by technicians will utilize wireless communications to communicate with the field devices. These communication elements that facilitate ITS device and center communications can be considered critical to modern transportation system operation.

Due to constraints regarding time and possible limited accessibility to devices in the target environment, not all deployed systems in the ITS environment will be included in the test scope. The DOT determination of critical ITS functions and information flows over communications links will prioritize the scope of ITS penetration testing. In all penetration tests, not every system is targeted. Rather the testing focuses on systems with unique or representative critical elements. If not previously defined by the DOT, we recommend an operational criticality analysis performed by the managers and operations personnel of the ITS using the NIST guidelines mentioned above. The PT scope should include the more critical functions and supporting systems determined by the analysis. Testing will be directed to components representing critical elements. ITS penetration test activity can be performed in phases, such as targeting Field components at chosen locations coordinated with law enforcement and conducting penetration testing targeting Center systems in a separate phase when the internal DOT resources to support the testing are different.

Selection of ITS functions and implementation for testing can be based on the DOT management concerns relative to ITS attack exposure. For example,

- Can the DMS messages be altered or manipulated by unauthorized parties or individuals?
- Are any ITS systems visible or accessible from the Internet? From the DOT Enterprise network? From the City's guest Wi-Fi network? Is the DOT Enterprise network accessible from the ITS network?
- How much of the ITS infrastructure can be accessed from a single Field location access point or interface?
- Does access to any single Center or Support system provide access to unauthorized control of other systems or field devices?
- Do any support contractor or vendor access paths and procedures allow unauthorized access to other ITS systems or DOT Enterprise resources?
- Can anyone with DOT Enterprise network access gain access to ITS resources and networks?
- Are all ITS wireless network access points protected from unauthorized modification?
- Is unauthorized activity at field equipment cabinets detected? Is the activity investigated to determine what activity and changes were performed during unauthorized access sessions?

ITS continue to evolve through capabilities supporting connected vehicles and new functions supported by increased communications with vehicles and travelers. Ideally new technology and services can be examined in test environments. Even when results of focused testing is available, the DOT PT can identify any gaps in the local ITS configuration and administration.

The majority of ITS deployments include legacy equipment with less functionality and cyber security protections. An ITS PT should address infrastructure components with different configurations or different manufacturers, especially when the devices provide the same function but may be deployed in different areas or locations.

3.2 Penetration Test Type

A penetration test can be categorized by at least three factors: penetration tester knowledge of the DOT ITS deployment and operation; DOT control and interaction with testers during the PT; access and authorizations provided by DOT to testers. In the literature, the combinations of the three factors have been labeled with colors relative to the target, “Box”, in the set below.

- Black Box – Testing where the testers performing the tests have no inside information and are executing the tests as would be performed by an external bad actor attacker. Test results will represent what penetration can be expected by *any* independent threat source. Only some attacks on externally detected vulnerabilities may be successful, dependent on the resources applied by the attacker, so this approach is least helpful for DOT risk estimations.
- Gray Box – The testers have partial knowledge of the target networks, systems and applications. Represents the typical threat agent with good reconnaissance techniques and access to information via the Internet. Permits better selection of attack paths seeking to exploit critical function vulnerabilities.
- White Box – The testers are given all pertinent documentation concerning the target networks, systems and applications. Focused attacks are selected to uncover potential vulnerabilities. The White Box test type provides the most comprehensive results across the broadest spectrum of attack paths. The prior information provided the testers reduce the effort to collect it through reconnaissance, permitting more time to select and execute attacks. This test type provides the most understanding of existing exploitable vulnerabilities and mitigation recommendations and is recommended when the testing schedule is a consideration. When the PT schedule is constrained to duration and schedule, this approach eliminates activity not contributing to the objectives.

Use Gray Box Testing

Providing independent penetration testers with the most information about the ITS deployment and operations yields the greatest depth of vulnerability identification and impact estimates, giving the DOT the broadest view of risks to remediate.

Most DOT PT engagements will achieve risk reduction objectives with a Gray Box type penetration test, the best type for agencies conducting comprehensive testing for the first time. A White Box test approach provides the most insight into risks from current vulnerabilities in the target ITS. A Black Box approach is appropriate for operational field device testing where manufacturer product details may not be available.

Another variant for the Pen Testers is the Red Team, consisting of a DOT internal group with penetration test expertise but managed by another part of the DOT organization[6]. Typically, the Red Team performs

[6] Red Teams for large organizations may contract with external organizations for testers with particular technical expertise.

Gray Box type tests, with some knowledge of the target environment, but the DOT ITS management and operations are not informed of the test execution. In some cases, the DOT management is informed only of the test findings and required mitigations. Red Team testing is more likely to uncover deficiencies with Operations and procedures, especially with response to unexpected security events.

3.3 Adversary Models and Tester Selection

The DOT should consider the types of adversaries to model for an ITS PT. In the context of risk assessment, the adversaries are termed threat agents. The potential adversaries for the DOT locality ground transportation system will cover a range of capabilities, motivations and objectives as listed in Table 1.

Table 1 Transportation System Adversary Types

Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud, manipulate transportation services and implement ransomware. These groups pose a threat to transportation systems through their ability to hire or develop hacker talent.
Foreign services	Foreign services are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the critical infrastructures that support military power - impacts that could affect the daily lives of U.S. citizens across the country.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. The worldwide population of hackers poses a relatively high threat of attempting an isolated or brief disruption causing serious damage to transportation systems during major events.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.

Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. During large public events, disruption of transportation systems provides high value to meeting terrorist objectives.

Although a DOT may not consider foreign agents or terrorists as likely attackers for relatively small locality transportation systems, we recommend planning for ITS PTs applying the attack techniques and capabilities of the more sophisticated adversaries for two reasons. First, the transportation system and ITS of a small locality can become a valuable target during a major event such as sports, entertainment, or other public celebration. Therefore, the set of potential adversaries will expand beyond those expected to target the local or regional community transportation systems. Second, the experienced outside organizations performing penetration testing in multiple industries can utilize resources and techniques as capable as the more sophisticated attackers, so the PT results will provide a more complete view of vulnerability impacts to the DOT ITS.

Assume the Worst Adversary

Use Penetration Testers capable of performing attacks expected from the very capable and determined adversaries. Use the context of a major public event when considering transportation impacts.

Performing penetration testing requires expertise and specialized software and hardware tools to uncover weaknesses in device and systems configurations and operations. Although penetration testers spend time identifying potential attacks to compromise the ITS, penetration testing is not “ethical hacking” or similar activities described in public literature. A DOT should not consider contracting with expert “hackers” to conduct an ITS PT. Test execution should be planned to minimize impacts to public transportation. Penetration attempts as simple as demonstrating unauthorized changes to traffic signals, such as turning them off, have shown that individual driver reactions will be unpredictable; some drivers stopping while others drive through an intersection at the speed limit. Attacks with the potential of causing irreversible damage to the target ITS or the public can be performed in an isolated test environment. When the PT is conducted on the operating ITS, the attack sequence can be modified to avoid or minimize the damaging situation. In order to provide a test report with recommended mitigations to prevent the successful attacks, the penetration testers and organization need to draw from knowledge of ITS system design and applicable security controls, technical and operational, and frame mitigations to allow the DOT to plan enhancements in the context of DOT risk reduction. This perspective is unlikely to be available from hackers.

3.4 Test Environment

When planning the deployment of new enhanced ITS systems and components, equipment may be staged in a test environment for integration testing with existing legacy systems for functional testing, equipment configuration verification, and refining operations procedures. The testing environment provides a better environment for penetration testing of device protections and impacts from disruptive attacks. Penetration testing in this environment uses focused resources, tends to take less time and involves fewer impact concerns. The risk impact from the attacks is significantly less than the same attacks performed in the deployed operational ITS. However, the scope of testing conducted in a test environment is limited to the functions, interfaces and operations procedures matching the planned deployment configuration and may not faithfully represent the production environment. It is important to note that active penetration testing, by its nature, invasive to ITS resources. Although the penetration test team can utilize methodologies to mitigate this impact, it needs to be understood that testing can have a negative effect on the ITS environment being tested. Awareness and communications between stakeholders during testing help to reduce this negative impact.

Use Test Environments When Available

Use a test environment when the PT scope matches. When the scope requires using the deployed ITS, use Rules of Engagement and coordination with local government agency POCs throughout the planning and execution to control impacts.

When the DOT does not have a separate ITS test environment with the critical functions and supporting systems, PTs must be executed on the operational ITS. Minimizing impacts to the operational ITS requires controls in four areas of the PT plan.

- Specifying controls on PT activity to minimize unexpected attack event consequences disrupting traffic flow through specifying applicable test assumptions and Rules of Engagement and permitted test methods.
- Establishing in the PT communications plan the methods, contact information and responsibilities for coordinating activity awareness (daily schedule) and response to attack consequences.
- Inclusion of a locality law enforcement POC in planning and execution of the PT activities when there exists any potential to disrupt local transportation.
- Daily “after action” review of PT activity to identify any additional controls following daily testing.

One benefit of penetration testing in the live ITS environment is evaluating DOT ITS operations response and management to intrusion. When evaluating security operational response, the DOT needs to determine the extent of prior PT test activity awareness provided to operations teams relative to the fidelity of response results. Actual penetration attempts of the localities transportation system and ITS usually do not come with prior notice. When evaluation of security operations detection and response to unauthorized activity is one of the goals of an ITS PT, some awareness of the PT by Center operations leadership will reduce risk of unexpected disruption while providing a realistic view of response effectiveness.

4 Defining the Penetration Test Plan

Internal DOT and external stakeholder buy in, such as law enforcement and local government agencies, will benefit from a concise document describing the ITS Penetration Test Plan. In addition to describing the objective, penetration test type and environment described in Section 3, the PT Plan should describe the management responsibilities and execution so all stakeholders understand the ITS PT activities. A review of a draft PT Plan will provide stakeholders with the opportunity to voice any concerns with the test controls and impacts of the testing.

A template ITS Penetration Test Plan is included in the Appendix. The following sections provide recommendations and options for the ITS PT Plan sections. The next sections describe the plans and activities recommended for successful execution of the ITS penetration test with minimal unintended consequences or disruptions.

PT Plan Template

The ITS Penetration Test Plan template provides a comprehensive starting point for identifying the "things to do" when planning an ITS Penetration Test.

4.1 Test Management

Successful penetration testing driving DOT priorities for associated risk mitigations requires the PT management taking account of applicable stakeholder priorities during a PT engagement. The PT management activities can aide the transition from successful test execution to applying resources to priorities for recommended mitigations for the target ITS.

The stakeholders for a DOT ITS PT will vary depending on the size of the locality and interaction with external systems and services outside the DOT jurisdiction.

The level of DOT staff effort to support an ITS PT will vary based on the availability of supporting ITS documentation, ITS system deployment and operations SME, ITS infrastructure and operations in the PT scope. At minimum, an organization authoritative program manager, project manager, applicable system and operations SME, and facilitators for monitoring hands-on testing will need to be available throughout the PT effort with management and SME more involved in the planning and reporting stages, whereas cybersecurity, project management staff and responsible facilitators more involved throughout the PT execution. A representative ITS PT involved approximately 100 person-hours of effort for one DOT where a project manager or DOT SME accompanied the PT testers throughout a 2-week on-site test activity in addition to time required for planning and analysis of results. The amount of hours DOT expended during on-site testing can be reduced to several hours if DOT staff involvement is limited to daily morning tailgate calls with the PT testers.

4.2 Management Interfaces

Sometimes a PT will uncover unexpected vulnerabilities or impacts to the ITS and local transportation. Taking an "expect the unexpected" approach to PT management is recommended in establishing the DOT functional organization POCs for engagement communications and decision making. From the safety perspective, including contacts with local government agencies such as law enforcement is necessary for every operational ITS PT.

The ITS PT Plan template includes a section to record all the authorized stakeholder POCs, facilitating communications throughout the PT execution.

4.3 Recommended Controls

The DOT penetration test objectives, policies and operational target environment constraints will motivate some controls and constraints on the ITS PT. Section 3.1 of the ITS Penetration Test Plan template provides sample assumptions to tailor regarding penetration testing activities of a DOT's ITS infrastructure. When contracting with an external penetration testing organization, the PT assumptions and execution controls should be included in contract Statements of Work.

Document PT Assumptions

Include in the PT Plan document all applicable assumptions of the DOT organization responsible for the ITS and security as well as the Penetration Testers.

4.4 Communication Plan

The authorized stakeholder representative POCs for test status, change management and activity coordination should be listed and disseminated to all PT project staff. The PT Plan should document the types, modes and frequency of ITS PT engagement communications.

Test plan execution status should be communicated through stakeholder status calls as required. Frequency of status reviews should be daily, especially when tests are executed in the locality ITS and targeting field devices and operations.

The communication plan should include requirements that the PT team will immediately notify the stakeholder representatives POC if testing has an inadvertent impact on the test environment, if a vulnerability is discovered that subjects the locality agency to immediate risk of compromise, or an active compromise is detected.

Communications Key to PT Success

All ITS PT stakeholders and penetration test project members need to know the POCs and the PT status reviews during testing execution. Be prepared to communicate plan changes and unexpected results to stakeholders.

When new vulnerabilities are discovered with use of ITS vendor products and software, the DOT PT managers need to report the vulnerabilities to the ITS vendor or supplier and the US CERT Coordination Center (CERT/CC). The DOT ITS vendors will have customer support methods to follow reporting vulnerability issues with products. In addition, report an IT vulnerability at https://www.us-cert.gov/report or to CERT/CC at https://www.kb.cert.org/vuls/report . OT product vulnerabilities can be reported via email to NCCICCUSTOMERSERVICE@hq.dhs.gov or call 1-888-282-0870. The ITS PT Plan should identify the DOT personnel responsible for submitting appropriate vulnerability reports to the vendors and these agencies.

4.5 Change Management

All proposed changes to the PT plan, including testing scope, test team members, test activity and activity schedule, should be reviewed and mutually approved by the appropriate DOT and penetration test organizations. The PT stakeholder POC must be notified of any change requests due to problems with the test environment, equipment, tools or interruptions to live systems. Communicate all changes to the designated PT project POC specified in the PT Plan Section 3. Changes to test activity times or locations of live ITS systems should be communicated to the Law Enforcement and any other external locality POC. The Plan and a record of change activity for one PT engagement will shape the planning of future PT engagements.

> **Be Prepared for Changes**
>
> Establish an approval process for any required or requested changes to the PT Plan such as scope or test methods.

4.6 Data Collection and Management

A variety of test equipment will be used during penetration test activity and test case execution. All test case results and raw data should be stored encrypted on persistent storage such as laptop hard drives or network storage systems. Access to penetration test analysis data by DOT stakeholders outside of the Penetration Test team should be managed through the Penetration Test organization primary POC.

The DOT should specify control and retention requirements for all PT data collected by the Penetration Test organization in the contract or statement of work for the project. PT results should be treated as sensitive, confidential and proprietary DOT information and protected according to DOT information protection policy.

> **PT Results are Sensitive**
>
> Control storage and dissemination of PT tests and results of attacks as very sensitive information. Apply protections according to DOT information protection policy.

4.7 Technical Review Meeting

A technical review meeting should be scheduled with DOT SME and the Penetration Test organization team at least 2 weeks prior to the start of the field testing. The purpose of this meeting is for the SMEs and Penetration Testers to discuss all aspects of the DOT ITS environment covered in the provided documentation about the DOT ITS. For White Box testing, useful documents include

- ITS network architecture
- ITS equipment installed
- Purpose of equipment in use
- Types of access needed to in-scope systems
- Communication protocols
- Network configurations

- Network access controls
- DOT Security policies.

This meeting is expected to answer any questions that may arise from the documentation review for the test team to have a full understanding of the ITS environment prior to the start of the field testing. Gray and Black box test types will involve exchange of less information about the target ITS infrastructure. The meeting is recommended to allow the DOT representatives to bring up concerns or any planned system changes or public events scheduled during the testing. It should be noted that more than one call may be necessary to conduct a comprehensive technical review of a large, complex DOT ITS with external communications.

4.8 Test Readiness Review

A Test Readiness Review (TRR) provides concurrence amongst stakeholders that the proposed tests provide representative coverage, the test environment is operational for testing and key preconditions are met to support testing. The TRR is the formal meeting where all stakeholders agree that they are ready to conduct the penetration test according to the Test Plan. A one-sheet approval form is recommended to record approval by authorized representatives of the DOT and test organization to proceed with testing. When the scope of the ITS PT is narrowly focused, the TRR can be a short status meeting ending with a consensus to start testing.

Always Conduct a TRR

The TRR provides stakeholder concurrence that all controls and communications are in place to start testing and avoid undesired surprises impacting locality transportation.

4.9 Schedule

The time required to plan, conduct and report an ITS PT will depend on many factors such as complexity and scope of ITS infrastructure, diversity of manufacturer equipment, extent of communications infrastructure and interfaces, DOT policies, available DOT personnel resources, and events in the locality impacting deployed ITS testing. DOT internal policies and processing can vary across agencies. So, a rough estimate of time to complete a DOT ITS PT engagement with field testing and reporting could range from three months to a year for phased testing of a complete ITS serving a large city or region.

A minimal PT schedule, in terms of weeks, including some device testing in a lab, is included in Section 3.3.5 of the ITS PT Plan template. The template schedule starts following management approval to engage the PT organization team to conduct the test. This approval process for the project will vary across DOT agencies. The plan assumes lab testing and remote penetration tests of the ITS occurs prior to DOT onsite testing. Durations and tasks for obtaining external stakeholder participation, particularly law enforcement, will vary across localities. The template schedule does not include a specific milestone for external approvals although the DOT should plan to have them by the Test Readiness Review milestone.

Following the TRR, any changes to schedule due to availability of equipment, personnel, environmental factors or other locality operational ITS constraints should be reflected in an updated schedule communicated to all stakeholders.

The template schedule assumes a moderate amount of testing for the four test method types described in Section 5.1. However, the schedule template does not include an estimate for conducting social engineering testing.

5 Selecting Penetration Testing Methods and Controls

The penetration test relies on a cooperating team of cybersecurity experts who examine opportunities to exploit weaknesses in the deployment of cybersecurity controls in applications, control systems, communications, networks, telematics systems, roadside infrastructure and vehicle on-board equipment. In general, functional or compliance test plans document the specific test cases to be performed on the test subject or system. The exploratory nature of penetration testing - hunting for a weakness, gaining access or privileges, exploring what unauthorized activity or information is available, followed by looking for the next target - involves creativity from the tester, flexibility and real-time adjustments to attack procedure. Thus, the penetration tester cannot be expected to document specific test cases for each target beyond test types or general methods prior to starting testing.

Determining opportunities to discover vulnerabilities open to threats to the ITS environment starts with review and analysis of:

- Security policies, practices and procedures,
- Physical access controls, redundancy and monitoring,
- Remote access controls,
- Networking topologies and inventory documentation,
- Network segmentation,
- Firewall policies and logical access controls,
- Communication protocols between ITS systems and
- Physical component systems and related firmware.

> **ITS Mix of Technology Requires Multiple PT Methods**
>
> Use of IT and OT technology and system operations requires examining existing DOT security program controls for the ITS and applying a comprehensive set of methods to uncover existing vulnerabilities open to attack.

A significant portion of the ITS environment review is expected to occur with DOT Subject Matter Experts (SMEs) on the technical review exchanges prior to field testing as described in section 4.7.

5.1 Test Methods

Penetration tests are based on many factors, such as technology versions, configurations, hardening, running services, network access controls, facilities and operations. There is no way to enumerate all tests that will be performed and there may be tests *listed below* that are later discovered as not applicable in the field. Penetration testing is dynamic and highly dependent on what is found in the ITS environment. For this reason, a test team may not follow exactly what is listed in a PT Plan. However, all tools and methods used throughout the PT should be documented in the final report submitted to the DOT (see Section 7).

5.1.1 Physical Penetration Test

The major objective for a physical penetration test is to ascertain the strength of existing physical security controls and uncover weaknesses before attackers can discover and exploit them. The focus for the ITS physical penetration testing should be the field equipment:

- Advanced Transportation Controller (ATC)
- Data communications equipment
- Environmental ITS Sensors
- ITS Roadway Payment Equipment
- ITS Traffic Signs
- Malfunction Management Unit (MMU)
- Roadside Unit (RSU)
- Surveillance Cameras (CCTV)

Include Physical Penetration Testing

Conduct for new and legacy Field equipment, especially vendor products without independent verification of security controls or appropriate DOT operations policies.

Physical penetration testing can be directed to the Center facility location of ITS systems if the facilities and locations have not been tested through broader DOT security assessments. For example, Center management systems may be deployed in a data center facility with other DOT IT systems and equipment. Facility security assessments may not examine the control of access to ITS resources within the data center or management of ITS access privileges. In this case, inclusion of physical penetration tests to centralized systems and supporting resources should be included in the ITS PT.

RSUs scattered throughout a locality are often not under surveillance and protected only by generic locks installed by the cabinet manufacturer. The keys to those RSUs are available for purchase on the open market. Once attackers open the enclosure, all the equipment inside are completely accessible to them. They can replace or install their own equipment so that the whole cabinet comes under their control. The importance of physical security of these cabinets cannot be overstated.

Below are representative examples of physical access tests to include in an ITS PT.

- Assess device locations and any surrounding physical deterrent for accessibility,
- Examine the surrounding area of ITS equipment and cabinets for exposed cables,
- Attempt to unlock ATC cabinet through unconventional means, such as by lock pick,
- Inspect ITS devices and ATC cabinets for tamper mechanisms,
- Determine if the Traffic Management Center (TMC) is alerted to unauthorized tampering of devices or unauthorized opening of roadway cabinets and measure response time.

5.1.2 Embedded Hardware and Firmware Penetration Test

> **ITS Hardware & Firmware Testing**
>
> Few ITS components have independent cybersecurity evaluations. This testing requires a Lab environment and specialized tools. Candidate for a DOT Consortium sponsor so PT results can be available to all DOTs. Include in PT scope new vendor equipment without available independent testing of security controls.

Embedded hardware and firmware penetration tests are often performed in a lab environment on ITC equipment. The equipment may be subjected to non-invasive and invasive tests. While the former does not damage the equipment, this is not the case for invasive tests; the equipment could possibly be destroyed. Hardware and firmware testing often require expensive tools like JTAG test tools, wiring rework stations, logic analyzers and wideband scopes. Because of the amount of resources involved and expensive ITC equipment destroyed, DOTs could consider joining forces to form a consortium to perform a set of tests that are common among the DOTs. Embedded hardware and firmware tests could be one of these common tests.

For embedded hardware and firmware penetration tests, the test team will seek to identify and exploit weaknesses and vulnerabilities related to the field endpoint embedded system circuitry, hardware interfaces, on-chip debugging functions, bootloaders and firmware. In the lab, the test team will seek answers to, but not limited to, the following question. If the equipment is stolen from the field, can attackers:

- Extract keys and credentials,
- Circumvent tamper controls,
- Evade detection to modify firmware,
- Defeat secure bootloader,
- Evade detection to alter configuration,
- Disable logging and alarm mechanism or erase logs,
- Install backdoors in the system to allow remote control,
- Compromise the upgrade process,
- Exploit physical ports, for example, plugging in a WiFi dongle to enable wireless remote access and subsequently control the hardware from a nearby location.

5.1.3 Wireless Communication Penetration Test

The primary objective of wireless analysis is to gain visibility into wireless traffic, validate over-the-air security controls, and discover security weaknesses that enable an adversary to take remote control of a field device, alter its state, make it unavailable to system operators, falsify information, or attack back-end systems and servers without physically touching a device. The test team will determine if there are weaknesses in the encryption, whether the session is vulnerable to session hijacking and replay attacks and whether rogue RSUs can masquerade as legitimate to collect tolls and sensitive information. Often this test is performed on a production network and care must be taken not to disrupt its normal operation. In-depth analysis of wireless captures can also be conducted in a lab environment in parallel with any field testing.

> **Inadequate Wireless Protections Provide Path to Remote Attack**
>
> The ITS Communications subsystem use of wireless network technologies must be examined for exploitable vulnerabilities. Penetration Testing the field network wireless implementation can uncover inadequate data confidentiality leading to unauthorized access to the ITS infrastructure.

Tools typically used by Penetration Test organization in this type of testing include, but are not limited to:

- Spectrum and Signal Analyzer,
- RF Vector Signal Generator,
- Waveform Generator and
- Software such as RF Signal Generation Software and Audacity.

Test equipment and software used could be expensive, so this is another candidate for consortium testing as mentioned in the previous section.

5.1.4 Network Penetration Test

The test team will seek to identify and exploit vulnerabilities in the Wireless and Wired Networks that interconnect DOT ITS field devices with Support and Center management and control applications. This testing focuses on perimeter and compartment defenses, edge routers and gateways, and means to access backend compartments from field networks, internal data networks and remote access.

The test team will employ both passive methods such as a review of router configuration and firewall policies, and active approaches to actually carrying out attempts to exploit known vulnerabilities, identifying reachable hosts, versions of operating systems deployed, ports and services on the hosts to determine if they are necessary services. Unnecessary services on hosts increase the attack surface and create more vulnerabilities. The testers will identify unencrypted sessions to determine if they carry sensitive information such as passwords and whether they are vulnerable to session hijacking and man-in-the-middle attacks.

> **ITS Network Testing**
>
> The ITS Communications subsystem and supporting network technologies touch the entire ITS infrastructure. Penetration Testing the network for vulnerabilities is critical to determining the adequacy of network protections.

A penetration test organization uses a variety of open source, commercial and proprietary software tools such as:

- Network scanner
- Host scanner
- Vulnerability scanner
- Firewall policy analyzer
- Packet capture
- Password crackers
- Man-in-the-Middle Proxy
- Packet manipulation tool.

5.1.5 Application and Management Software Penetration Test

The test team will seek to identify and exploit weaknesses and vulnerabilities in head-end management server applications, business support systems in the Center environment as well as client application software that interfaces management servers. Activities include testing for OWASP Top 10 Web Application Security Risks in web-based systems, service-oriented architectures, and web services interfaces in support components such as databases, authentication services, crypto services, name services and time services. For client applications, the test team will reverse engineer the executables to bypass authentication, escalate privileges and extract keys and credentials. If databases are used by applications, the team will alter the data to exploit the application. Application penetration tests have special importance if an application is running on a shared computing environment, e.g., a laptop is shared by a group of field technicians on shifts and certain operations can only be performed by the supervisor of the group. The test team will explore if there are ways to gain supervisory privileges by a non-supervisor.

Penetration Test organization uses open source, commercial and proprietary tools in this type of testing such as:

- Web application vulnerability test tool
- Man-in-the-Middle Proxy
- Packet capture
- Password cracker
- Port scanner
- Reverse engineering tool
- Database tools

5.1.6 Social Engineering

The main objective of Social Engineering is to extract confidential information through psychological manipulation of people to exploit human weaknesses. Social engineering is a frequent avenue of attack initiation for any IT or OT target. Attempts are made to gain unauthorized access to system and application information, account credentials or process information permitting the attacker to gain privileges to perform additional attack steps. Social engineering penetration testing can be performed on-site and off-site. On-site tests may include:

- Pretending to be an employee by wearing the company's uniform or using a duplicated ID,
- Pretending to be a delivery person to access security areas,
- Pretending to be a guest and access network connections in a conference room,
- Deliberately "forgetting" and leaving a USB thumb-drive containing a Proof of Concept executable on an employee's desk.

Off-site tests may include:

- Calling the hotline to impersonate an employee who forgets her password and having it reset to a known one;
- Sending phishing emails or SMS to employees with links to files containing malware;
- Dumpster diving, looking for sensitive information in printouts and documents thrown in the trash.

Social engineering involves a large amount of work and preparation. At minimum, the ITS penetration test should include a review of the DOT HR security plan and associated DOT policies. However, vulnerabilities uncovered through social engineering are not specific to an ITS attack. Usually any ITS vulnerabilities gained through social engineering steps indicate general gaps in physical security, staff security awareness, training and implementation rather than gaps specific to the ITS.

Social engineering testing as part of an ITS PT will be valuable when an ITS is operated, administered or maintained by outside contractors and the DOT does not have results or statements about security training minimizing successful social engineering attempts of contractor personnel. A number of recent attacks directed at electric utilities and the power infrastructure, attributed to foreign governments, involved use of social engineering to get utility contractors to perform unauthorized activity allowing successful penetration of utility resources [2] . To the extent the DOT business functions, people and management have not been assessed for social engineering risks, this attack activity is recommended for inclusion in the penetration test.

5.2 Security Domain Testing Matrix

An ITS may be composed of several subsystems and components as indicated in Figure 1. The ITS PT can apply multiple test methods to the technology underlying the ITS as described in Section 5. Table 2 illustrates a method of summarizing the penetration test coverage for the ITS. The table below depicts the matrix of security domain testing to be conducted on DOT ITS components. Across multiple PT engagements, a composite matrix facilitates tracking overall coverage of ITS PT activity and planning subsequent tests. The sampling of ITS components included in the table should be edited to reflect the

ITS PT Domain Dashboard

Use a tabular matrix to track ITS PT coverage across PT test domains, ITS subsystems and components, and PT projects.

DOT ITS. Enhancements to consider are designating components in scope of a PT engagement and grouping components by the DOT ITS architecture subsystem names.

Table 2: Security Domain Testing Matrix

Component	Physical Penetration	Embedded Hardware / Firmware	Wireless	Network Penetration	Application & Management Software
Network Switches	No	Yes	No	Yes	Yes
TMC Web App 1	No	No	No	Yes	Yes
TMC Web App 2	No	No	No	Yes	Yes
TMC Servers	No	No	No	Yes	No
Traffic Control Systems	No	No	No	Yes	Yes
RSU	Yes	Yes	Yes	Yes	Yes
ATC Controller	Yes	Yes	If Applicable	No	Yes
MMU	Yes	Yes	No	No	No
ITS Traffic Signs	Yes	Yes	If Applicable	No	No
Sensors	Yes	Yes	If Applicable	No	No
ITS Smart Lights	Yes	Yes	If Applicable	No	If Applicable
Radios	Yes	Yes	Yes	Yes	Yes
CV RSE	Yes	Yes	Yes	Yes	Yes
CCTV	Yes	Yes	If Applicable	No	No
IP Encoder	Yes	Yes	Yes	No	No
<additions such as Vehicle components>					

6 Specifying the Rules of Engagement

An initial recommended Rules of Engagement for ITS Penetration Tests is included in Section 4 of the PT Plan template in the Appendix. Topics recommended for inclusion are

- Disclosure statements about intent to minimize risk exposures from the penetration testing, use of scanning and locations, caveat that penetration testing has potential to disrupt the target environment, and establishing contingencies for recovery.
- DOT responsibilities for obtaining approval from all applicable stakeholders to conduct the test, informing stakeholders of potential and actual security breaches, establishing POC and lines of communication during testing, information about the DOT and ITS to be supplied to the penetration test organization and support to be made available to the penetration testers.
- Penetration Tester responsibilities for abiding by restrictions set forth by DOT, handling DOT provided equipment for on-site and off-site testing, conducting non-destructive testing (if applicable), not conducting Denial of Service tests (if applicable) or Social Engineering tests, the extent to which exploits are followed to determine extent of impacts.

At the start of the project, the ITS PT participating test parties should sign a Mutual Non-Disclosure Agreement (MNDA) on the use and disposal of confidential information released by the DOT organization and collected by the PT organization.

The Rules of Engagement can include controls on personnel accessing DOT resources, time when testing can be conducted, the targets, any changes permitted to ITS resources and required authorizations, accounts and privileges provided for testing and authorization to change settings.

Spell out the PT Rules of Engagement

PT Rules of Engagement need to state all the DOT and Penetration Test organization responsibilities throughout the PT planning, execution and reporting of results. Example rules are included in the ITS Test Plan template.

Another important engagement rule concerns confidential handling of discovered vulnerability information, the attack execution and the impacts discovered by the penetration testers.

With regard to actual attack methods and penetration test tools, the recommended approach is to specify in the Rules of Engagement the pre-determined tools to be used by the penetration testers so the DOT SMEs can request more details to understand use and potential impact, or constrain tools and techniques known to significantly disrupt the ITS systems and target environment.

A DOT may not want to authorize use of three attacks or techniques for a PT:

1. Denial of Service attacks
2. Use of social engineering techniques.

If the DOT does not use a comprehensive, updated and monitored anti-virus solution for all desktops, user devices and applicable host systems, as well as a policy controlling use of mobile media (USB sticks, etc.), then the risk of malware introduction in the ITS is high enough to assign resources to address the gap across the Enterprise. If the programs are in place for the DOT but policies are not applied to the ITS, mitigations should be examined without the need to conduct a PT with test cases attempting introduction of malware.

Unless the DOT has a separate test environment with an operational ITS, Denial of Service (DoS) attacks on a locality ITS will cause disruption with unpredictable impacts. In the Rules of Engagement, limit DoS attacks to PTs in test environments.

The DOT and penetration test organization should mutually refine the PT rules prior to starting the engagement. If operational factors such as events in the locality, resources unavailable, or surprising test results drive changes to testing scope, the Roles of Engagement defining how the PT is conducted can be updated with concurrence of the authorized stake holder representatives. Signatures on the PT Test Plan document section update is worth the effort to demonstrate stakeholder agreement.

7 Requesting Reports of Results

The DOT should request an ITS PT Report documenting all details of the ITS PT execution, targeted ITS components, exploited vulnerabilities and attack findings. The Report should document attacks and results with enough detail and fidelity to allow the DOT to repeat the attack in the future and verify subsequent risk mitigations to prevent repeated attack success.

PT Report Documents a Baseline

The Penetration Test Report needs to provide enough detail to facilitate repeating the test to measure improvement in cybersecurity protections over time.

Vulnerabilities in ITS system software and device configurations should use open industry standard scoring scales such as the NIST National Vulnerability Database Common Vulnerability Scoring System (CVSS) version 3 to assign severity scores to system software, firmware vulnerabilities findings identified during the PT[7]. The CVSS scores rank the criticality of vulnerabilities regarding potential impact. The DOT Penetration Test findings CVSS numeric score provides IT managers, vulnerability bulletin providers, security vendors, application vendors and researchers a common language of scoring ITS vulnerabilities. ITS vendor products and software vulnerabilities exploited during the penetration test may have assigned identifiers, CVSS scores, and remediation assigned by U.S. Computer Emergency Readiness Team (US-CERT) or the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). The DOT infrastructure managers should be monitoring the CERT Cybersecurity and Infrastructure Security Agency (CISA) vulnerability advisories[8] and the NIST Information Technology Laboratory National Vulnerability Database (NVD) for common vulnerabilities in the DOT ITS vendor products[9].

Request Standard Scoring of PT Findings

Require the Penetration Test organization to apply CVSS scores of vulnerability severity for each PT finding.

PT exploited vulnerabilities rooted in inadequate policy and procedures can be assigned severity scores based on penetration tester and industry experience seeing the impacts across industry testing of a range of IT and OT systems. For example, successful attacks taking advantage of weak or default account credentials can permit a broad range of ITS impacts depending on the role or functions performed by the targeted systems. Impacts from use of weak authentication credentials such as passwords due to insufficient policy or enforcement has appeared in the Center for Information Security (CIS) Top 20 Critical Security Controls for Effective Cyber Defense for many years.

[7] Current and previous versions of the CVSS standard and on-line training is available from the Forum of Incident Response and Security Teams at https://www.first.org/cvss/ and NIST's website at: https://nvd.nist.gov/vuln-metrics/cvss .

[8] The CISA security alerts are available at https://www.us-cert.gov/ncas/alerts

[9] The searchable NVD is available at https://nvd.nist.gov/

In order to plan DOT ITS cybersecurity risk reduction efforts to mitigate successful penetration attacks, the impact of the attack and severity of the vulnerabilities exploited in the attack need an objective, repeatable rating. As discussed in Section 2.1, risk ratings provide a means for the DOT to prioritize mitigation efforts to address the most severe vulnerabilities with highest potential negative impacts creating risk for the DOT and the locality population. A risk assessment will identify relative risk to the DOT of demonstrated successful attacks by considering all of the types of impact, including safety, and the likelihood of attacks over time. The PT Report of Results documents attacks that can occur under the conditions of the test. A risk assessment uses the successful exploits to estimate likelihood of attack occurrence and total impact to the DOT when calculating risk ratings.

PT Report Needs to Identify Risks

Require the Penetration Test organization to document all of the tests performed, evidence of the outcome, an independent rating of associated vulnerability severity, and an assessment of ITS attack impact and associated risk.

An ITS risk assessment is a separate activity from the PT involving a broader review of transportation management policies, regulatory requirements, historical operations and both safety and security events. The historical record is used to estimate likelihood of attacks to the transportation infrastructure involving the ITS and resulting damage. A DOT risk management program will establish the framework and methods for categorizing risks associated with the ITS vulnerabilities identified by the PT. An independent PT organization can estimate threat likelihood and transportation impacts from prior DOT assessment engagements. Similarly, the penetration testers can evaluate the elevated risk associated with the exploitation of combinations of multiple minor ITS vulnerabilities that enable attacks causing a significant transportation exposure. The DOT risk management program can determine appropriate risk reduction efforts for the DOT transportation mission by considering including the demonstrated vulnerability exploits and impacts identified from the ITS PT. Working with the DOT risk managers is an important next step to acquiring necessary resources to address ITS vulnerabilities impact the DOT mission.

Involve DOT Risk Management

Require the Penetration Test organization to document all of the tests performed, evidence of the outcome, an independent rating of associated vulnerability severity, and an assessment of ITS attack impact and associated risk.

8 Next Steps - Mitigation Planning and Monitoring

DOT management will determine if the ITS PT engagement was successful relative to the success criteria discussed in Section 2.3. The DOT agency needs to evaluate the successful penetration events, the exploited vulnerabilities and the recommendations for mitigations from the penetration testers. The rated severity and risk from the ITS vulnerabilities should be mapped to the overall DOT risk profile.

The penetration testers provide recommended mitigations to prevent successful ITS attacks or minimize the impacts. The DOT will analyze the root causes for the successful penetration attacks, identifying vulnerabilities due to weaknesses in processes and procedures. The corrective actions may involve the broader DOT policies and procedures beyond the ITS or DOT IT management.

Remediate and Lower Risk

The DOT must determine the root causes for successful ITS attacks and weigh the penetration tester view of risk against the DOT risk profile. Resources must be allocated to the mitigation efforts applicable to the DOT ITS critical functions based on risk.

Plan a follow on PT to include determining the effectiveness of the remediation efforts.

The DOT should create mitigation project plans for the vulnerabilities permitting unauthorized access and activity with the critical ITS functions and components. Mitigation plans need completion dates to drive resource management to address risk reduction activity.

The DOT should evaluate ITS mitigation effectiveness through follow-up penetration re-testing and additional testing as appropriate when the mitigations change the infrastructure or operations. Re-testing should repeat those attacks targeting the root cause vulnerabilities, facilitating verification of risk reduction and absence of changes introducing new vulnerabilities.

9 Conclusion

The purpose of this document is to facilitate DOT organization efforts to use ITS Penetration Testing for successful reduction of risks with use and operation of an ITS. Penetration testing can identify vulnerabilities and impacts with ITS systems and technology. Identification of mitigations to successful ITS penetrations enable the DOT to direct actions to maintain resilient ITS are designed, installed, operated, and maintained to survive a security incident while sustaining critical functions of a DOT.

With systematic planning and execution, ITS penetration testing can uncover exploitable vulnerabilities in the ITS infrastructure and operations and provide estimates of risk impacts from unmitigated weaknesses. A valuable activity of a DOT or any organization relying on Operations Technology and Information Technology is conducting managed penetration testing of the ITS for awareness of successful attacks not prevented or mitigated with the target ITS deployment.

While DOT ITS deployments vary in size and complexity, the ITS Penetration Test planning and execution involves the same structure and activities, tailored to the objectives, scope and execution constraints of each locality penetration test engagement. The DOT management can structure the security management program encompassing the ITS to use periodic PT engagements with continuous monitoring of risk reduction to achieve ground transportation risk reduction for the DOT localities.

10 References

[1] Patrick O'Neill. Ransomware Is Putting a Damper on Our Smart City Future. Gizmodo, May 14, 2019. https://gizmodo.com/ransomware-is-putting-a-damper-on-our-smart-city-future-1834731404

[2] Rebecca Smith, Rob Barry. America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It. Wall Street Journal, Jan. 10, 2019.

[3] National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1, April 16, 2018. https://duckduckgo.com/l/?kh=-1&uddg=https%3A%2F%2Fnvlpubs.nist.gov%2Fnistpubs%2FCSWP%2FNIST.CSWP.04162018.pdf

[4] U. S. Department of Homeland Security. Transportation Systems Sector Cybersecurity Framework Implementation Guidance. June 26, 2015. https://www.dhs.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf

[5] U. S. Department of Energy. Cybersecurity Capability Maturity Model (C2M2), Version 1.1. February 2014. https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf

[6] U. S. Department of Transportation. Penetration Testing Concepts for Intelligent Transportation Systems. April 2019.

[7] Council of Registered Security Testers (CREST). A guide for running an effective Penetration Testing programme. April 2017. http://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf

[8] The PTES Team. The Penetration Testing Execution Standard Documentation, Release 1.1. February 8, 2017. http://www.pentest-standard.org/index.php/Main_Page

[9] The PTES Team. The PTES Technical Guidelines. http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

[10] ISECOM, Open Source Security Testing Methodology Manual (OSSTMM 3). http://www.isecom.org/research/osstmm.html

[11] Open Web Application Security Project (OWASP). Testing Guide 4.0. August 3, 2015. https://www.owasp.org/index.php/OWASP_Testing_Project

[12] National Institute of Standards and Technology. NISTIR 8179 Criticality Analysis Process Model: Prioritizing Systems and Components. April 2018. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8179.pdf

[13] National Institute of Standards and Technology. NIST Special Publication 800-30 r1, Guide for Conducting Risk Assessments. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

11 Appendix - ITS Penetration Test Plan Template

Introduction

The Appendix provides a template for the topics and content recommended to include in an Intelligent Transportation System (ITS) Penetration Test Plan. This template includes all the topics and sections recommended for communicating the ITS penetration test plan to the governing Department of Transportation (DOT) organization (hereafter, AGENCY) stakeholders. Since ITS vary in size, complexity, management and external connectivity, section contents need to be tailored to the target ITS and purpose of the penetration test.

In the introduction, identify the penetration test formal contract or work order, requesting organization and penetration testing supplier engaged to perform the penetration test of the governing organization (hereafter, AGENCY) ITS in <geographic LOCATION>.

Document Organization

Provide a brief description of the contents of the document sections. For example,

1. **Scope of the Test** - describes the AGENCY ITS infrastructure; the critical operations and supporting components; the components and operations to be examined in the penetration test.
2. **Penetration Test Overview** - identifies test assumptions; test objectives; test management and stakeholder representatives; test schedule; and penetration test methods included in the penetration test.
3. **Rules of Engagement** - states general disclosures about the testing and specific rules for the AGENCY, test organization and testing.
4. **Conclusion** - summarizes the test objective, execution and planned reporting of results.

Acronyms

At minimum, Include a list of acronyms to faciliate reading by those unfamiliar with ITS, cybersecurity or penetration testing terms. The following list of acronyms are used in this template. *Note the template plan text follows the style recommendation of introducing the acronym on first occurrence in the full body text*.

ATC Advanced Transportation Controller

ATMS Advanced Traffic Management Systems

CCTV Closed Circuit Television

CERT Cyber Emergency Response Team

CLI Command line interface

COTS Commercial off-the-shelf

CV Connected Vehicle

DAA	Detect and avoid
DMS	Dynamic Message Signs
DMZ	DeMilitarized Zone (network)
DoS	Denial of Service
DOT	Department of Transportation
DSRC	Dedicated Short-Range Communications
EVS	Emergency Vehicle Subsystem
ICS	Industrial Control Systems
ITS	Intelligent Transportation System
LPD	Location Police Department
MMU	Malfunction Management Unit
MNDA	Mutual Non-Disclosure Agreement
ONU	On-Board Unit
PENTESTORG	Company/Internal Organization contracted to perform a penetration test
PIAS	Personal Information Access Subsystem
PMS	Parking Management Subsystem
POC	Points of Contact (individual)
RAM	Random Access Memory
RF	Radio Frequency
RSE	Road Side Equipment
RSU	Road Side Unit
RTS	Remote Traveller Support
SME	Subject Matter Experts
SQL	Structured Query Language
TCS	Toll Collection Subsystem
TMC	Traffic Management Center
TRVS	Transit Vehicle Subsystem
USDOT	United States Department of Transportation
V2X	Vehicle to Infrastructure
VMS	Video Management Systems, Variable Message Signs

Scope of Test

The scope of the penetration test assessment includes devices, applications, networks, access controls, communications and configurations that comprise the AGENCY ITS infrastructure. This test plan outlines the types of tests that will be carried out by the test team, identifies the points of contact for the penetration test, and begins to lay out procedures and guidelines necessary for the assessment.

The goal of the penetration test is to identify exploitable vulnerabilities in the AGENCY ITS infrastructure, illustrate harmful impacts from attacks taking advantage of the vulnerabilities and to recommend mitigation actions. Testing will be performed on site within the AGENCY ITS [deployed or test] environment [and offsite at PENTESTORG facilities]. At the end of the project, a final report will be submitted to the AGENCY Department of Transportation (<AGENCY acronym>) that summarizes all findings, with associated vulnerability ratings and recommended actions for remediation.

AGENCY ITS Architecture

As shown in the United States Department of Transportation (USDOT) National ITS Reference Architecture in Figure 1,[10] there are five (5) subsystems in an ITS implementation that are common among transportation agencies and corresponding systems. They are the Center, Support, Field, Traveler, and Vehicle subsystems. Each of these areas serve as critical functions to the Intelligent Transportation System infrastructure. The communications configuration, which includes access controls, encryption, protocols, redundancy and paths between these areas is a sixth critical component in the infrastructure. Due to the constant need to improve and upgrade ITS systems with emerging technology, current ITS implementations consist of both legacy and new technology. The test plan template includes representative elements of selected subsystems as well as both the legacy and the new technology within those subsystems. The penetration test plan should present the AGENCY ITS environment within the context of the standard architecture facilitate communication with other organizations within and outside the AGENCY.

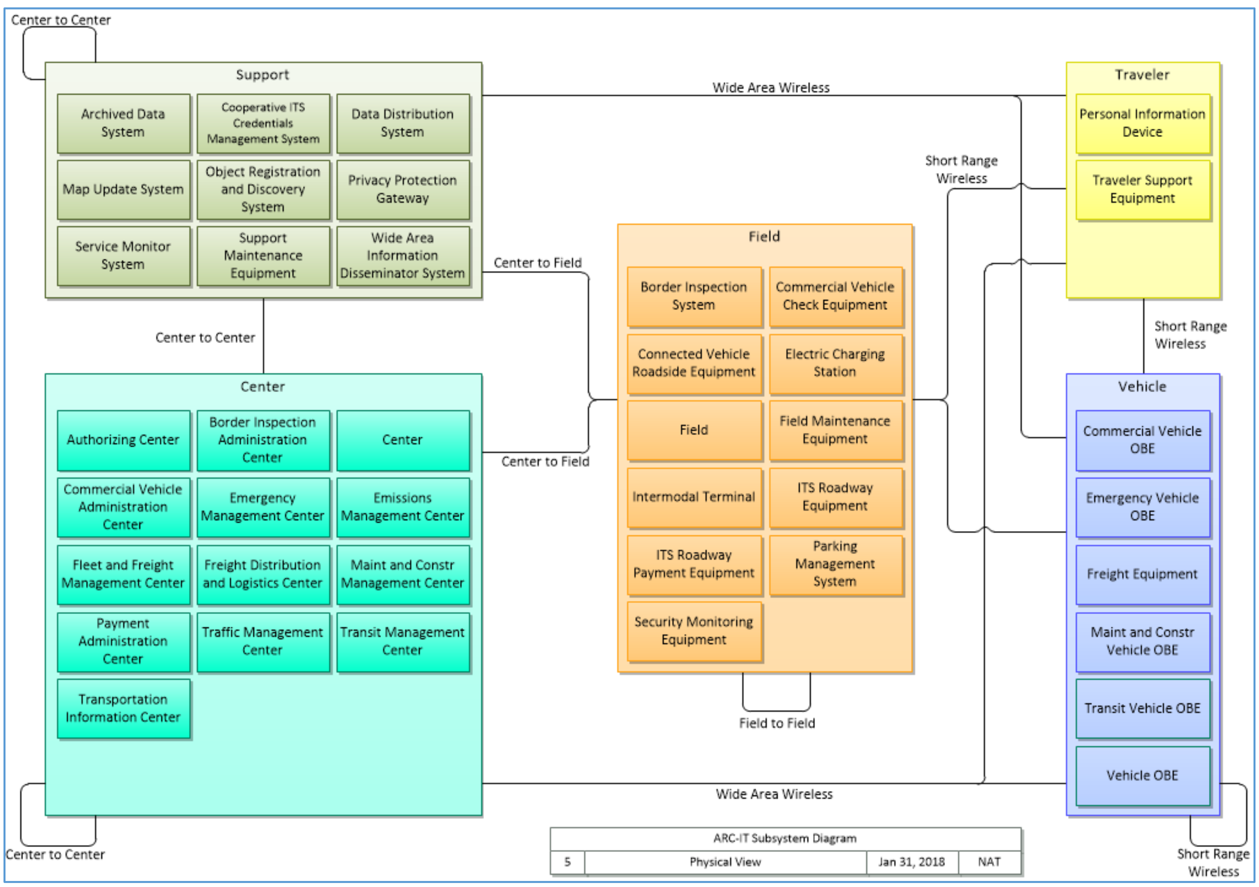

Figure 2: ITS Physical Architecture – Enhanced Systems Connections View

[10] The United States Department of Transportation National ITS Reference Architecture. 2018. URL: https://local.iteris.com/arc-it/html/viewpoints/physical.html

The diagram can be highlighted to illustrate the areas not currently supported by the subject ITS or not included in the penetration test scope. In addition, the architecture should include links to Regional ITS and connected systems when the AGENCY ITS is part of a larger regional system.

Critical Operations and High-Value Targets

This section will be updated to reflect the AGENCY specific ITS infrastructure. The AGENCY ITS logical architecture of systems and components can be depicted in a Figure with indication of the elements in scope for the penetration test. Providing a summary of the entire deployed ITS gives context for considering the AGENCY systems and functions supporting critical operations.

Example critical operations to include:

- Center – Describe the functions and systems deployed in the AGENCY Transportation centers, such as personnel and systems that monitor and manage the Intelligent Transportation System at a specified location. It also consists of the networking that supports ITS systems. Indicate critical components of the center to include the personnel, networking, server systems, and web applications associated with Center-to-Field and Center-to-Center interactions.
- Support – Describe the AGENCY operations and systems that serve non-transportation purposes, such as communications, security, or management. Describe the critical components of the AGENCY Support center such as the server systems and web applications associated with Center-to-Field and Center-to-Center interactions.
- Field – Describe the AGENCY Field subsystem devices in proximity to the road network that function as surveillance (e.g. traffic sensors, Closed Circuit Television (CCTV) cameras), traffic control (e.g. traffic signal controllers), public messaging (e.g. Dynamic Message Signs (DMS)), and toll collection (e.g. parkway tolls, parking). Describe the AGENCY critical Field components such as traffic signaling, the public messaging system, the surveillance system and the wireless and wired networks that support them.
- Traveler – Describe the AGENCY Traveler subsystem consisting of equipment used by a person traveling the public roadways to access public transportation services (e.g. emergency notifications, real-time public transit schedules).
- Vehicle – Describe the AGENCY supported commercial and non-commercial vehicles of various sizes, and cargo, as well as the on-board electronic systems such as navigation. Include critical components including onboard devices that generate and receive data with ITS services.

In addition to the previous five areas, the communications between them are critical.

- Communications – The AGENCY communication components of the ITS can consist of very diverse wired and wireless technologies that may include WiFi[11], WiMAX[12], MDS™ [13] and cellular

---

[11] WiFi is a trademark of the WiFi Alliance which means IEEE 802.11x
[12] WiMAX is a trademark and service mark of the WiMAX Forum
[13] MDS™ is a Trademark of General Electric Company

networking. They can utilize encrypted or non-encrypted access controls and protocols. Include AGENCY field maintenance utilizing wireless communications to communicate with the field devices. All of these communication elements that facilitate ITS device and center communications can be considered critical.

If the AGENCY has performed a criticality analysis for safety or security, include a summary of the analyses and AGENCY ITS components supporting critical operations.

Components in Scope

AGENCY and PENTESTORG will determine what device types, which devices and field locations will be included in the penetration test. For initial penetration tests, devices with different configurations or different manufacturers should be included, even if the devices serve the same purpose (for example different vendor Advanced Transportation Controllers (ATC).

Refer to the AGENCY ITS architecture Figure to illustrate the area components in scope relative to the AGENCY ITS architecture.

<Insert DOT ITS Logical Architecture Figure(s)>

The following components of the ITS have been deemed critical and are expected to be a major focus of this penetration test. Update the template components to include the components deployed within AGENCY's ITS environment and within scope of the penetration test. Add manufacturer and model or product name and version. Most of the devices will be tested within the AGENCY production network and any component where lab testing is believed to be more suitable can be identified as such. AGENCY and PENTESTORG will decide which test setting is most appropriate for each component. For the applicable tests in scope refer to section 3.4 Test Methods below.

Center Components

- General
    - Network Switches –
    - Routers –
    - Firewalls –
    - Intrusion Detection Systems –
    - Authentication Systems -
- Traffic Management Center (TMC)
    - Advanced Traffic Management Systems (ATMS) -
    - Web Application 1 -
    - Web Application 2 -
    - Servers -

- Adaptive Traffic Control Systems –
- Video Management Systems (VMS) –
- Ramp Metering Systems -

Support Components

- ITS Asset and Maintenance Management –
- Support Maintenance Equipment –
- Object Registration and Discovery System –
- Data Distribution System –
- Archived Data System -
- Map Update System –
- Service Monitor System –
- Wide Area Data Disseminator System
- Privacy Protection Gateway –
- Cooperative ITS Credentials Management System -

Field Components

- ITS Roadway Equipment
    - Advanced Transportation Controller (ATC) –
    - Traffic Controller Cabinets -
    - Malfunction Management Unit (MMU) –
    - Variable Message Signs (VMS) –
    - ITS Detection Sensors –
    - Changeable/Dynamic Message Signs (CMS/DMS) –
    - Emergency Vehicle Pre-emption (EVP) -
    - ITS Smart Lighting –
    - Radios and Road Site Units (RSU) -
    - Connected Vehicle (CV) Roadside Equipment (RSE) –
    - Speed Feedback Signs –
    - Battery Backup Systems -
- Toll Collection Subsystem (TCS) –

- Parking Management Subsystem (PMS) -
- Security Monitoring Equipment
  - CCTV Camera Systems –
  - IP encoder –

Traveler Components

- Mobile Applications -
- Remote Traveler Support Subsystem (RTS) –
- Personal Information Access Subsystem (PIAS) -

Vehicle Components

- Connected Vehicle -
- Vehicle Subsystem (On-board Unit (ONU) –
- V2X Connected Applications -
- Emergency Vehicle Subsystem (EVS) –
- Transit Vehicle Subsystem (TRVS) -

Communications Network ITS

- ITS Network Components
  - Communications Systems (voice+) –
  - Network Switches (managed) –
  - Network Switches (unmanaged) –
  - Routers –
  - Firewalls –
  - Intrusion Detection Systems –
  - Wireless Systems –
  - Center to Center Communications –
- ITS DeMilitarized Zone (DMZ) Components

  List the Communications Network, Web Proxy and server components used for interfaces to external entitities.

Penetration Test Overview

The goal of the ITS penetration test is to identify security control gaps in the AGENCY ITS implementation in order to plan mitigations reducing the risks to operation of the deployed system before threat sources attempt to exploit the vulnerabilities. *Refine this sample description based on the AGENCY ITS PT goals.* The penetration test relies on a cooperating team of cybersecurity experts who examine opportunities to exploit weaknesses in the deployment of cybersecurity controls in applications, control systems, communications, networks, telematics systems, roadside infrastructure and vehicle on-board equipment. Penetration testing targets weaknesses in operations of the ITS including inadequate personnel, training, situational awareness of activity at Network and Security Operations Centers, and inadequate response to unauthorized and undesireable activity. Refine this description based on the coverage for the AGENCY ITS penetration test.

Determining opportunities to discover vulnerabilities open to threats to the AGENCY ITS environment starts with review and analysis of:

- Security policies, practices and procedures,
- Physical access controls, redundancy and monitoring,
- Remote access controls,
- Networking topologies and inventory documentation,
- Network segmentation,
- Firewall policies and logical access controls,
- Communication protocols between ITS systems and
- Physical component systems and related firmware.

Edit this list based on the scope of the penertration test and the actual AGENCY documentation exchanged with the PENTESTORG. Describe previously conducted vulnerability assessments of the AGENCY infrastructure such as the enterprise IT infrastructure and applications and the extent of inclusion of the ITS.

A significant portion of the review is expected to occur with AGENCY Subject Matter Experts (SMEs) and PENTESTORG SMEs on the technical review call(s) prior to field testing as described in Section 3.3.4.

Test Assumptions

This section provides a concise list of assumptions regarding the penetration test agreed to by the AGENCY and PENTESTORG. Usually the assumptions are generated in earlier planning meetings between the AGENCY and PENTESTORG. The list in this template contains assumption examples used in other penetration test engagements of AGENCY ITS. Edit the list based on the ITS Penetration Test engagement.

The following assumptions are made regarding penetration testing activities of AGENCY's ITS infrastructure:

- The AGENCY will supply documentation to PENTESTORG that will include the ITS network architecture, applications, field networks, user manuals, equipment and security controls.
- Prior to testing, at least one conference call between AGENCY Subject Matter Experts (SMEs) and PENTESTORG shall be scheduled to review the ITS network architecture, applications, field networks, equipment and security controls, and to bring up any concerns or any planned system changes scheduled during the assessment. Refer to section 3.3.4 for more information. The conference call(s) may include third party SMEs if components in scope are managed/administered by contractors, managers, or cloud service providers and deemed necessary by AGENCY and PENTESTORG.
- Application credentials for management systems will be provided by AGENCY.
- AGENCY and PENTESTORG will select applications that are identified to be mission critical for the management and monitoring of the AGENCY ITS infrastructure. Selection criteria to be considered include:
    - Both AGENCY and third party developed applications,
    - Interactive and automated processes,
    - Communication with both backend servers and field devices, and
    - Network accessibility of application.
- All applicable components and services not directly accessible via the Internet will require special VPN access or internal network connectivity for PENTESTORG and will be provided by AGENCY.
- AGENCY will authorize PENTESTORG equipment, including Penetration Testing laptops, to be connected to the AGENCY network infrastructure as required for testing.
- AGENCY will authorize PENTESTORG access to buildings and field locations as required for testing.
- AGENCY will provide the test team with intersection maps consisting of associated devices and device information to adequately prepare for field assessment.
- AGENCY will provide test team with network and device mapping.
- AGENCY will supply required documentation, including user guides and security policies, for any in scope devices, application and systems.
- AGENCY will provide test team with two <components> currently deployed at AGENCY prior to the field assessment (for lab testing).
- Before the testing begins, AGENCY will conduct backups of the target systems and network configurations as it deems necessary.

- AGENCY will be prepared to reconstitute tested systems should the systems be corrupted due to testing activities.
- AGENCY IT personnel will actively monitor for potential service degradation.
- AGENCY will supply a point of contact during testing for questions, notification of critical findings or notification of system impact.
- AGENCY will provide the test team with a point of contact throughout the onsite test assessment for device or center access.
- AGENCY will coordinate with the LOCATION Police Department (LPD) ahead of field testing to allow for the test team to access roadway devices, if applicable.
- AGENCY will provide any additional assistance required by the test team to access field equipment, e.g. bucket trucks for access to roadway equipment on gantries (if necessary), LPD coordination for partial road closure (if necessary) for safe device access.
- If any systems are managed by third parties, AGENCY will coordinate authorization for the penetration test team to perform any required testing on those systems and AGENCY will provide a direct point of contact for that third party in case any questions or issues arise.
- Any application changes relevant to ongoing testing will be issued in a separate addendum. Any addendums will be supplied by AGENCY to the penetration test organization.

Test Objectives

The objective of this ITS system penetration test is to identify the exploitable vulnerabilities through attack sequences in the AGENCY ITS environment and to recommend mitigations for successful penetrations and ITS unauthorized manipulations. All security findings and recommendations for remediation will be documented in a final report that PENTESTORG will develop and submit to the AGENCY at the closing of the project.

Details for penetration test method objectives specific to each test scenario are found in the Test Methods Section 3.4.

Test Management

The following points of contact will be supporting the penetration test assessment at AGENCY. Document all the relevant AGENCY, PENTESTORG, and any additional stakeholder representative Points of Contact (POC). Example roles are included in Table 1 and should be edited based on the AGENCY Penetration Test.

AGENCY Department of Transportation Team – Test Organization					
	Name	**Role**	**Desk Phone**	**Mobile Phone**	**Email**
Primary Point of Contact		ITS Manager			
Field Point of Contact		DOT Network Engineer			
IT Point of Contact		CISO			
IT Point of Contact		Cybersecurity Analyst			
IT Point of Contact		Cybersecurity Analyst			

PENTESTORG Project Management					
	Name	**Role**	**Desk Phone**	**Mobile Phone**	**Email**
Primary Point of Contact		Principal Investigator			
Escalation PoC		Program Manager			
Alternate Point of Contact		Technical Manager			

PENTESTORG Technical Pen Test Team					
	Name	**Role**	**Desk Phone**	**Mobile Phone**	**Email**
Point of Contact		Test Team Lead			
Point of Contact		Security Analyst			
Point of Contact		Security Analyst			
Point of Contact		Security Analyst			

External Agency Coordinators					
	Name	**Role**	**Desk Phone**	**Mobile Phone**	**Email**
Primary Point of Contact		Project Manager			

Table 3: Points of Contact

Communication Plan

Table 1 will be the authorized points of contact for test status, change management and activity coordination.

Test plan execution status will be communicated through stakeholder status calls as required.

Change Management

All proposed changes to the test plan, including testing scope, test team members, test activity and activity schedule, will be reviewed and approved by the AGENCY and PENTESTORG. The points of contact will be notified of change requests due to problems with the test environment, equipment, tools or interruptions to live systems. All changes will be communicated to the designated point of contacts listed in Table 1.

Data Collection and Management

A variety of test equipment will be used during the penetration test activity and test case execution. All test case results and raw data will be stored encrypted on persistent storage such as laptop hard drives or network storage systems. Access to penetration test analysis data by AGENCY stakeholders outside of the PENTESTORG team will be managed through the PENTESTORG primary POC.

Technical Review Call

A technical review call shall be scheduled with AGENCY Subject Matter Experts (SMEs) and PENTESTORG at least 2 weeks prior to the start of the field assessment. The following paragraph is applicable to a "White Box" penetration testing approach where the testers are given all pertinent documentation concerning the target networks, systems and applications, and offers results that are more thorough. The documentation exchange and topics discussed in the Technical Review call will be more limited for "Gray Box" or "Black Box" approaches (see [REF]).

PENTESTORG requests that AGENCY provide documentation about the ITS network architecture, applications, field networks, user manuals, equipment and security control with a sufficient amount of time to review before a technical review call is scheduled. The purpose of this call is for the SMEs and PENTESTORG to discuss all aspects of the AGENCY ITS environment covered in the provided documentation, including but not limited to:

- ITS network architecture,
- ITS equipment installed,
- Purpose of equipment in use,
- Types of access needed for in-scope systems,
- Communication protocols, and
- AGENCY Security policies.

This call is expected to answer any questions that may arise from the documentation review in order for the test team to have a full understanding of the ITS environment prior to the start of the field assessment. The session provides the AGENCY an opportunity to bring up concerns or any planned system changes scheduled during the assessment. It should be noted that a number of calls may be necessary to conduct this comprehensive technical review for a full scope ITS penetration testing effort.

Testing Schedule

The execution of this penetration test will take place on-site at the AGENCY {test environment or deployed location(s)} {and off-site at PENTESTORG facilities}. Edit as appropriate for the penetration testing engagement.

A Test Readiness Review (TRR) provides concurrence amongst stakeholders that the proposed tests provide representative coverage, the test environment is operational for testing and key preconditions have been met to support testing. The TRR will be held with all stakeholders to concur with start of testing.

The estimated testing schedule for the Penetration Test and report delivery is shown in Table 2 below. Adjust the test week durations based on ITS scope of systems, operations and localities in scope for the penetration test.

Task	Estimated Test Week	Corresponding Dates
AGENCY Delivers ITS Infrastructure Documentation	1	
PENTESTORG Reviews Delivered ITS Documentation	2	
Initial Technical Review Call with AGENCY ITS Infrastructure and PENTESTORG Subject Matter Experts (SMEs)	3	
Test Readiness Review (TRR), authority to start testing	3 - 4	
Conduct Hardware and Firmware Penetration Testing on systems, devices at PENTESTORG Facilities	4-6	
Conduct Application and Management Software Penetration Testing Remotely (if applicable)	4-6	
Conduct Physical Penetration Testing On-Site	7	
Conduct Hardware and Firmware Penetration Testing On-Site	7	
Conduct Wireless Communication Testing (Done in parallel if on-site and other facility (lab) testing)	8	
Conduct Network Penetration Testing On-Site	8 - 9	
Conduct Application and Management Software Penetration Testing On-Site	8 - 9	
PENTESTORG Analyzes Test Results	9 - 10	
Draft Test Report Deliverable	11 - 12	
Final Test Report Deliverable	13 – 14	

Table 4: Estimated Test Schedule

Test Methods

As described in the ITS architecture, an ITS uses standard IT computing resources, applications, purpose built connected devices, with wired and wireless communications. Penetration test methods target weaknesses using attacks aimed at vulnerabilities in all quadrants of the technology and configuration. In addition, penetration attacks can target weaknesses in operations procedures and supporting personnel. An ITS PT should examine opportunities to exploit any vulnerabilities across all quadrants.

Penetration testing is dynamic and highly dependent on what is found in the ITS environment, and for this reason the test team may not follow exactly what is listed in this Test Plan document. All tools and methods used throughout the test assessment, however, will be documented in the final report and submitted to the AGENCY. The Template section is updated based on the scope, goals and PENTESTORG contractual agreement.

11.1.1 Physical Penetration Test

The test team will verify that strong physical security methods are applied in the field to prevent pedestrians or malicious agents from accessing AGENCY ITS roadway equipment. The equipment in focus are devices necessary for the primary function of the ITS system, such as a Roadside Unit (RSU), Advanced Transportation Controller (ATC), Malfunction Management Unit (MMU), Environmental ITS Sensors, ITS Traffic Signs, and Surveillance Cameras (CCTV).

Below are representative examples of physical access tests PENTESTORG will conduct. For this test, the team will:

- Assess device locations and any surrounding physical deterrent for accessibility,
- Examine the surrounding area of ITS equipment and cabinets for exposed cables,
- Attempt to unlock ATC cabinet through convential (key) and unconventional means, such as by lock pick,
- Inspect ITS devices and ATC cabinets for tamper detection mechanisms
- Verify that the Traffic Management Center (TMC) is alerted to unauthorized tampering of devices or unauthorized opening of roadway cabinets.

When Center and Support resources are located in facilities shared with other systems, describe whether the facilities and locations have been tested through broader AGENCY security assessments. If facility security assessments did not examine the control of access to ITS resources within a data center, include physical penetration tests to centralized systems and supporting resources.

Embedded Hardware and Firmware Penetration Test

The test team will seek to identify and exploit weaknesses and vulnerabilities related to the field endpoint embedded system circuitry, hardware interfaces, on-chip debugging functions, bootloaders and firmware. Testing of the devices, expected to be provided by the AGENCY prior to field testing (see Section 3.1) will be performed offsite at PENTESTORG test facilities and the rest of the device tests will take place onsite in the AGENCY's environment. The test approach will be {Black box} testing - this method of testing is where the testers performing the tests have no inside information about the device deployment, and are executing the tests as would be performed by an external bad actor attacker. Edit the representative examples of hardware and firmware tests PENTESTORG can conduct on provided ITS components.

Offsite at PENTESTORG test facilities, the test team will perform the following activities for the provided ITS devices. In the AGENCY environment, the test team may be limited in time and accessibility so only a subset of the tests will be performed on accessible field devices, indicated with an <u>underline</u> of the test activity.

- <u>Conduct Reconnaissance</u>: Conduct public information reconnaissance and analysis to gather information, such as Industrial Control Systems (ICS) Cyber Emergency Response Team (CERT) advisories and vulnerabilities identified from unpatched or fix-unavailable software, relevant to AGENCY ITS device firmware.
- Analyze Hardware Design: Examine the hardware and perform reconnaissance to identify processors, memory, programmable logic, secure components, onboard ports and connectors, debug interfaces, pad headers, unpopulated options.
- <u>Validate Security Controls</u>: Conduct testing to validate the existence and operation of the expected security controls:
  - Secure bootloader,
  - Firmware signature, and
  - Security event reporting.
- Analyze FLASH and RAM: Access FLASH storage and Random Access Memory (RAM) devices on the device. Attempt to access, download and decompose FLASH memory in search of security credentials, configuration information, firmware and device data.
- <u>Extract Credentials and Keys</u>.
- Redirect Code Execution.
- Defeat Secure Bootloader: Disassemble, analyze and attempt to defeat the secure bootloader and firmware integrity checks to install and run rogue code. For example, attempt to enable rogue code to run without manual intervention.
- Analyze Firmware and Create Rogue Firmware: Acquire, disassemble and analyze binary firmware. Modify firmware, reinstall modified code and attempt to execute rogue code.
- <u>Alter Device Configuration</u>: Assess the security of system variables and attempt to modify device configuration.
- Compromise Recovery/Firmware Upgrade Process.
- <u>Exploit Physical Ports</u>:
  - Disrupt communications between RSU and vehicle on board units,
  - Send crafted data to vehicle on board units,
  - Gain console access to the ATC,
  - Attempt to read and edit sensitive files,

        - Control a network of traffic signals,
        - Install corrupt traffic signal software,
        - Exploit internal storage,
        - Gain access to connected devices and
        - Verify that stored private keys, if used, are encrypted.
- Assess/Circumvent Tamper Controls.
- Employ Physical Attacks:
    - Determine whether an attacker can physically tamper with the device without detection.

List the tools to be used by PENTESTORG for this type of testing.

Wireless Communication Penetration Test

The following text provides a description of potential wireless tests to include in the ITS Penetration Test methods. Remove (or add) wireless testing not applicable to the target AGENCY ITS or out of scope for the penetration test engagement.

The PENTESTORG test team will seek to identify and exploit low-level vulnerabilities in wireless communications of field devices in the AGENCY wireless network(s) beginning with the modulation scheme and coding, media access control, link level properties, network synchronization, routing, and transport security up through application layer communication exchanges in wireless field networks and other wireless systems.

Since this testing will be performed on a {production} system, the test team will refrain from attempting active attacks on key ITS components and any active field tests will be conducted with customer approval. In-depth analysis of Radio Frequency (RF) captures will be conducted at the PENTESTORG facilities in parallel with any field testing. The testing approach for this area will be {Black box} testing - this method of testing is where the testers performing the tests have no inside information about the wireless deployment, and are executing the tests as would be performed by an external malicious attacker.

List the tools to be used by PENTESTORG for this type of testing.

Edit or replace the representative examples with the wireless tests PENTESTORG will conduct.

- Conduct Reconnaissance: Conduct public information reconnaissance and analysis to gather information available in the public domain, such as patent disclosures, ICS CERT advisories, and vulnerabilities identified from unpatched or fix-unavailable software relevant to AGENCY wireless communications.
- Perform RF Captures: Capture and analyze over-the-air exchanges using RF test equipment.

- Attempt to determine the use of secure wireless protocols over Dedicated Short-Range Communications (DSRC) and other utilized forms of wireless communication by performing an in-depth analysis of RF captures, in order to verify the use of strong encryption, authentication, integrity, and replay protection mechanisms.
- Exploit CV RSE/ITS Roadway Equipment WiFi Hotspot, if enabled:
  - Verify that the SSID is hidden and running over WPA2,
  - Attempt to access the network with default credentials, and
  - Attempt to access public internet through WiFi.
- Exploit CV RSE/ITS Roadway Equipment Bluetooth, if enabled:
  - Attempt to access the device by connecting via Bluetooth.
- Replay RF Messages to CV RSEs: Capture and replay over-the-air messages from the CV OBEs or back office centers (if applicable) or other CV RSEs (if applicable) toward the RSE to determine if the RSE handles duplicate packets or replay attacks.
- Replay RF Messages to ITS Roadway Equipment: Capture and replay over-the-air messages from the ITS sensors or other ITS Roadway Equipment (if applicable) toward the Roadway Equipment to determine if it handles duplicate packets or replay attacks.
- Replay RF Messages to CV OBEs: Capture and replay over-the-air messages from the CV RSEs to the CV OBEs to determine if the OBE handles duplicate packets or replay attacks.
- Manipulate and Inject RF Messages: Attempt to alter captured waveforms to determine if they are acted upon by CV RSEs, ITS Roadway Equipment and CV OBEs. If possible, attempt to represent falsified measurements from the field, and check if the crafted data was accepted by the TMC.

Network Penetration Test

The test team will seek to identify and exploit vulnerabilities in the Wireless and Wired Networks that interconnect Support and Center management and control applications and AGENCY ITS field devices. The network testing focuses on perimeter and compartment defenses, edge routers and gateways, and means to access backend compartments from field networks, internal data networks and external remote access. The testing approach for the network will be {White box –where the testers are given all pertinent documentation concerning the target networks, systems and applications, and offers results that are more thorough}.

List the tools to be used by PENTESTORG for this type of testing.

Below are representative examples of network tests PENTESTORG will conduct. *Note the examples refer to TMC and need to be edited for the ITS scope of the penetration test engagement*. This network penetration test may include:

- A review of equipment configuration and firewall policies, and fixed and wireless networks and transport system.
- Public information reconnaissance and analysis to gather information, such as ICS CERT advisories and vulnerabilities identified from unpatched or fix-unavailable software, relevant to AGENCY ITS network infrastructure.
- Passive analysis of traffic between components, including between the TMC applications and ITS Roadway Equipment, between ITS Roadway Equipment to other ITS Roadway Equipment and between TMC applications and servers to other TMC applications and servers:
  - Monitor and conduct traffic analysis on the system interfaces to assess information security,
  - Verify use of secure protocols and protocol versions,
  - Verify use of secure algorithms and other options,
  - Verify implementation and use of expected security controls and
  - Attempt to extract system and user credentials.
- Active scanning to:
  - Identify all hosts that are reachable from each of the networks (TMC applications and servers and Field devices),
  - Identify open network ports on these hosts,
  - Identify vulnerable service versions and missing patches,
  - Identify unnecessary services,
  - Assess the overall security hardening of the components and
  - Determine if access to a console in one device can allow the user to reach other devices on the network that the accessed device should not have access to.
- Active network testing:
  - Attempt to conduct man-in-the-middle attacks,
  - Attempt to replay, modify and manipulate messaging between systems, for example, between different ITS Roadway Equipment or between different TMC servers,
  - Attempt to inject upstream messages to affect, alter or disrupt systems and make unauthorized changes, for example, by spoofing the ITS Roadway Equipment and sending falsified data to the TMC to create fake alarms,
  - Attempt to inject downstream messages to affect, alter or disrupt systems and make unauthorized changes, for example, by spoofing the TMC and sending falsified data to the ITS Roadway Equipment to change traffic patterns,

- Attempt to gain unauthorized access or visibility into the AGENCY ITS environment networks via external means (e.g. the Internet),
- Attempt to gain unauthorized access or escalate privileges on permitted access to systems, and
- Attempt to circumvent access controls.

Application and Management Software Penetration Test

The test team will seek to identify and exploit weaknesses and vulnerabilities in head-end management server applications and business support systems in the Center environment. Activities include testing for Open Web Application Security Project (OWASP) Top 10 Web Application Security Risks in web-based systems, service oriented architectures, and web services interfaces in support components such as databases, authentication services, crypto services, name services and time services. The testing approach for this area will be White box – this method is where the testers are given all pertinent documentation concerning the target networks, systems and applications, and offers results that are more thorough.

List the tools to be used by PENTESTORG for this type of testing.

The team will conduct testing of management applications involved in {Center-to-Center and Center-to-Field} communications. Edit the representative examples of tests PENTESTORG will conduct. For this penetration test, the team will:

- Check for ICS CERT advisories and for known vulnerabilities in NIST's National Vulnerability Database.
- Test for OWASP Top 10 Web Application Security Risks.
- Test security configuration, including for downstream components.
- Analyze firmware update mechanisms.
- Attempt to gain access to system and user credentials.
- Attempt to grant permissions to an unauthorized user.
- Attempt to escalate user privileges.
- Attempt to exploit vulnerabilities in scripts and java-based components.
- Perform a Threat Evaluation: Conduct a high-level application threat evaluation to identify high value targets and potential goals and objectives of malicious actors.
- Validate Authentication Mechanisms: Identify weaknesses associated with the authentication mechanism (e.g., hardware security modules, hardware tokens, soft-certificates, User IDs and passwords) used to provide access to the Web-based application.
- Validate Authorization Mechanisms: Identify weaknesses associated with the authorization mechanism(s) and rate limiters used to restrict access to application functionality.

- Validate Design-Driven Security Controls: Validate the presence, proper operation and consistent use of design-driven application security controls and the remediation of known security weaknesses.
- Stress Application Logic: Identify weaknesses associated with the application logic and data flows, and user-input management and its impact on privileged and un-privileged functionality.
- Stress Middleware Logic: Identify vulnerable application software and underlying middleware, scripts or interactive programs that may be manipulated by an attacker to retrieve sensitive system information or compromise the security of the system.
- Analyze Server and Application Configuration: Identify weaknesses in the server and application configuration that can be used by attackers to compromise the security of the application, Web server or the underlying operating system.

Social Engineering

The main objective of Social Engineering is to extract confidential information through psychological manipulation of people. Social engineering involves a large amount of work and preparation. Include a review of the AGENCY HR security plan, particularly security awareness training and assessment, and discussion of its implementation. If broader security awareness training and assessment is not recent for personnel supporting the ITS operation, then include social engineering in the course of executing ITS penetration attacks.

Security Domain Testing Matrix

The table below depicts a summary of security domain testing to be conducted on each AGENCY in-scope ITS component. *Edit the list and values for the AGENCY ITS penetration test scope.*

Component	Physical Penetration	Embedded Hardware / Firmware	Wireless	Network Penetration	Application & Management Software
Network Switches	No	Yes	No	Yes	Yes
TMC Web App 1	No	No	No	Yes	Yes
TMC Web App 2	No	No	No	Yes	Yes
TMC Servers	No	No	No	Yes	No
Traffic Control Systems	No	No	No	Yes	Yes
RSU	Yes	Yes	Yes	Yes	Yes
ATC Controller	Yes	Yes	If Applicable	No	Yes
MMU	Yes	Yes	No	No	No
ITS Traffic Signs	Yes	Yes	If Applicable	No	No
Sensors	Yes	Yes	If Applicable	No	No
ITS Smart Lights	Yes	Yes	If Applicable	No	If Applicable
Radios	Yes	Yes	Yes	Yes	Yes
CV RSE	Yes	Yes	Yes	Yes	Yes
CCTV	Yes	Yes	If Applicable	No	No
IP Encoder	Yes	Yes	Yes	No	No

Table 5: Security Domain Testing Matrix

Rules of Engagement

The Rules of Engagement focus on the conduct and execution of the pentration test. The AGENCY and PENTESTORG may mutually refine these rules during the course of the penetration test engagement.

Disclosures

Any testing will be performed according to terms and conditions designed to minimize risk exposure that could occur during security testing. Scans may originate from the Internet, across AGENCY internal networks or from the localized subnet of the target systems.

Proactive contingencies will be used to ensure continuity of the environment during testing, such as backups and active monitoring.

The Rules of Engagement includes:

- The AGENCY will inform all management personnel who would be involved in informing any police or government authorities of a breach of security and make the personnel aware of the penetration test, the Execution Requirements and Rules of Engagement.
- The AGENCY will obtain approval from the AGENCY Subject Matter Experts, Asset Operators and Asset Owners, for purposes of the proposed assessment.
- The AGENCY will identify appropriate contacts for “24 x 7” communication during any testing.
- All testing will be nondestructive in intent.
- The PENTESTORG test team will abide by any penetration test restrictions set forth by the AGENCY, if applicable.
- PENTESTORG and the AGENCY will agree upon the extent to which discovered vulnerabilities are validated through proof-of-concept exploitation [based on the weight of available artifacts, the importance of the finding, and the potential risk to production systems].
- Any AGENCY supplied proprietary testing equipment will be returned in working condition.
- Any AGENCY ITS devices supplied for offline testing will be returned in working condition unless invasive testing is authorized by the AGENCY.
- During testing, if PENTESTORG determines in its sole judgment that the AGENCY’s assets or systems are at extreme risk of malicious exploitation, PENTESTORG will notify the AGENCY of such vulnerability immediately rather than wait until the end of the assessment. The AGENCY will then determine if further testing should occur before mitigations are considered and deployed.
- Assessment activities will not intentionally include Denial of Service (DoS) attacks unless specifically requested and appropriately authorized by the AGENCY.
- The AGENCY will provide information to PENTESTORG as warranted and appropriate *via* specific requests.

- All participating test parties will abide by the Mutual Non-Disclosure Agreement (MNDA) signed at the start of this project, with regard to the use and disposal of confidential information released by the AGENCY.
- Access to the AGENCY's network will be limited to personnel assigned to the penetration test, with user accounts and credentials protected appropriately. Network activities will be governed by the following constraints:
  - Assessment activities will not intentionally affect the availability of the AGENCY's network during normal business hours unless prior arrangements have been made and authorized by the AGENCY.
  - Assessment activities will not intentionally interfere with the AGENCY's ability to conduct business without prior authorization.
  - Assessment activities will not install, change, delete or alter any of the AGENCY's network technology without the prior permission of the AGENCY.
  - Assessment activities will only access the AGENCY's network when permitted by the AGENCY (e.g., *via* telephone, e-mail, prior service agreement).
  - All information discovered in the course of the proposed assessment while accessing the AGENCY's network shall be governed by the confidentiality provisions of the contract between the AGENCY and PENTESTORG that authorizes the performance by PENTESTORG of the proposed assessment.
  - Hours during which assessment activities may access the AGENCY's network will be determined and identified on a case-by-case basis. Accordingly, network accounts used by this effort will allow access to the AGENCY's network by PENTESTORG assigned personnel during the requested time periods.
  - Assessment activities will access the AGENCY's network by use of a distinct user account that provides for audit control and process tracking. This user account will conform to the AGENCY's established user account and password guidelines, and this user account will be given privileges as appropriate to support performance of the proposed assessment.
  - Assessment activities will ensure current anti-malware/virus protection is active on any assets used to access the AGENCY's network.

Security Testing Administration Includes

- The AGENCY and PENTESTORG will identify and agree on the list of specific target devices, applications and systems that will be the subject of the penetration test.
- A daily or weekly status briefing to discuss findings, progress and outstanding issues will be held at the request of the AGENCY contact.

- The test team may require support from multiple contacts. These include primary penetration test contact, location access contact, subject matter expert contacts, and network, security and application support contacts. The contacts are included in Table 1. *If there are third party vendors administering and maintaining elements of the tested environment, then the applicable vendor contacts are included in the table.*
- PENTESTORG will utilize safeguards including encryption to protect AGENCY data when in transit and when at rest.

Penetration Testing May Include

In support of the penetration testing activities included in Section 3.4, security testing may include the following activities:

- Port scans and other network service interaction and queries,
- Network sniffing, traffic monitoring, traffic analysis, and host discovery on wired and wireless infrastructure,
- Attempts to gain unauthorized remote access or visibility into the environment,
- Attempted logins or other use of systems, with any derived account credentials,
- Attempted Structured Query Language (SQL) injection and other forms of input parameter testing,
- Use of exploit code for leveraging discovered vulnerabilities,
- Password cracking via capture and scanning of authentication databases,
- Spoofing or deceiving servers regarding network traffic,
- Adding user accounts,
- Review and analysis of network topologies,
- Review and analysis of segmentation and access controls,
- Review and analysis of network, system and application configurations,
- Review and analysis of firewall configurations,
- Review and analysis of security policies and
- Enumeration, analysis and probing of physical hardware.

Penetration Testing Will <u>Not</u> Include

Testing will not include any of the following activities:

- Testing of network, devices, applications or system not specified as in scope,
- Changes to assigned user passwords unless approved by AGENCY,
- Modification of user files or system files,

- Telephone modem probes and scans (active and passive),
- Intentional viewing of AGENCY staff email, Internet caches, and/or personnel cookie files,
- Denial of service attacks,
- Exploits that will introduce new weaknesses to the system and
- Intentional introduction of malicious code (viruses, Trojans, worms, etc.).

Penetration Test Report

PENTESTORG will provide a preliminary PT Report on *<date>* with a final report following review and incorporation of AGENCY comments by *<date>*. Add any ITS PT Executive presentation if appropriate.

The PT Report will include all findings, interpretation of risk and impact, and mitigation recommendations based on the penetration testing. The PT Report will include

- Executive Summary, a management level overview of the key findings, an assessment of threat and risk, and top-level recommendations for remediation.
- Findings Overview, one or more matrices to summarize the findings. Each finding will be listed with a descriptive title, its severity rating, the applicable security domain, the objective observation/measurement, and as deemed appropriate the hardware, configuration, and firmware version of the component to which the finding applies.
- Scope and Methodology, describes the ITS components, the technical approach used to perform the test, and the risk assessment methodology to rate the findings.
- Test Environment, the configuration of the environment used to conduct the testing, the product model, software version, hardware version, and firmware of the components tested, as well as the test equipment and tools used by PENTESTORG.
- Detailed Security Findings by Domain presents the findings by security quadrant (e.g., Application and Management Software, Wireless Communications, Network Penetration, and Embedded Hardware and Firmware) with recommended mitigation(s).

Conclusion

The AGENCY Department of Transportation is conducting the ITS Penetration Test to gain insight into the exploitable vulnerabilities in the deployment and operation of the ITS.

The Penetration Test Plan provides an understanding of the ITS components that are in scope for this penetration test and the types of penetration test methods that will be conducted on those components. The management plan for execution of the penetration test and stakeholder points of contact are provided along with the estimated schedule for completion. The Rules of Engagement defined the constraints on execution of the penetration testing to minimize impacts to the AGENCY ITS.

References

Include DOT references for the ITS implementation and operations, policy or prior test reports and penetration testing references.

U.S. Department of Transportation
ITS Joint Program Office-HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487
www.its.dot.gov

FHWA-JPO-19-763

U.S. Department of Transportation