

## Protection of Transportation Infrastructure from Cyber Attacks: A Primer

### DETAILS

183 pages | 8.5 x 11 | PAPERBACK

ISBN 978-0-309-44308-1 | DOI 10.17226/23516

### AUTHORS

Countermeasures Assessment and Security Experts LLC and Western Management and Consulting LLC; National Cooperative Highway Research Program; Transit Cooperative Research Program; Transportation Research Board; National Academies of Sciences, Engineering, and Medicine

BUY THIS BOOK

FIND RELATED TITLES

Visit the National Academies Press at [NAP.edu](http://NAP.edu) and login or register to get:

- Access to free PDF downloads of thousands of scientific reports
- 10% off the price of print titles
- Email or social media notifications of new titles related to your interests
- Special offers and discounts



Distribution, posting, or copying of this PDF is strictly prohibited without written permission of the National Academies Press. (Request Permission) Unless otherwise indicated, all materials in this PDF are copyrighted by the National Academy of Sciences.

### **ACKNOWLEDGMENT**

This work was sponsored by the American Administration of State Highway and Transportation Officials (AASHTO), in cooperation with the Federal Highway Administration and the Federal Transit Administration (FTA) in cooperation with the Transit Development Corporation. It was conducted through the National Cooperative Highway Research Program (NCHRP) and the Transit Cooperative Research Program (TCRP), which is administered by the Transportation Research Board (TRB) of the National Academies.

### **COPYRIGHT INFORMATION**

Authors herein are responsible for the authenticity of their materials and for obtaining written permissions from publishers or persons who own the copyright to any previously published or copyrighted material used herein.

Cooperative Research Programs (CRP) grants permission to reproduce material in this publication for classroom and not-for-profit purposes. Permission is given with the understanding that none of the material will be used to imply TRB, AASHTO, FAA, FHWA, FMCSA, FTA, Transit Development Corporation, or AOC endorsement of a particular product, method, or practice. It is expected that those reproducing the material in this document for educational and not-for-profit uses will give appropriate acknowledgment of the source of any reprinted or reproduced material. For other uses of the material, request permission from CRP.

### **DISCLAIMER**

The opinions and conclusions expressed or implied in this report are those of the researchers who performed the research. They are not necessarily those of the Transportation Research Board, the National Research Council, or the program sponsors.

The information contained in this document was taken directly from the submission of the author(s). This material has not been edited by TRB.

## *The National Academies of* SCIENCES • ENGINEERING • MEDICINE

The **National Academy of Sciences** was established in 1863 by an Act of Congress, signed by President Lincoln, as a private, non-governmental institution to advise the nation on issues related to science and technology. Members are elected by their peers for outstanding contributions to research. Dr. Ralph J. Cicerone is president.

The **National Academy of Engineering** was established in 1964 under the charter of the National Academy of Sciences to bring the practices of engineering to advising the nation. Members are elected by their peers for extraordinary contributions to engineering. Dr. C. D. Mote, Jr., is president.

The **National Academy of Medicine** (formerly the Institute of Medicine) was established in 1970 under the charter of the National Academy of Sciences to advise the nation on medical and health issues. Members are elected by their peers for distinguished contributions to medicine and health. Dr. Victor J. Dzau is president.

The three Academies work together as the **National Academies of Sciences, Engineering, and Medicine** to provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions. The Academies also encourage education and research, recognize outstanding contributions to knowledge, and increase public understanding in matters of science, engineering, and medicine.

Learn more about the National Academies of Sciences, Engineering, and Medicine at [www.national-academies.org](http://www.national-academies.org).

---

The **Transportation Research Board** is one of seven major programs of the National Academies of Sciences, Engineering, and Medicine. The mission of the Transportation Research Board is to increase the benefits that transportation contributes to society by providing leadership in transportation innovation and progress through research and information exchange, conducted within a setting that is objective, interdisciplinary, and multimodal. The Board's varied committees, task forces, and panels annually engage about 7,000 engineers, scientists, and other transportation researchers and practitioners from the public and private sectors and academia, all of whom contribute their expertise in the public interest. The program is supported by state transportation departments, federal agencies including the component administrations of the U.S. Department of Transportation, and other organizations and individuals interested in the development of transportation.

Learn more about the Transportation Research Board at [www.TRB.org](http://www.TRB.org).

## Table of Contents

Preface.....	iv
Executive Summary .....	vii
Introduction .....	1
Chapter 1 Top Myths of Transportation Cybersecurity .....	4
Chapter 2 Cybersecurity Risk Management, Risk Assessment and Asset Evaluation .....	8
Chapter 3 Cybersecurity Plans and Strategies, Establishing Priorities, Organizing Roles and Responsibilities .....	38
Security Planning.....	38
APTA Recommended Security Program.....	40
Establishing Priorities .....	42
NIST Cybersecurity Framework .....	42
Defense in Depth Approach.....	46
Security Zones Approach .....	48
Attack Modeling .....	51
Organizing Roles and Responsibilities.....	52
Relationship with Physical Security .....	52
Chapter 4 Transportation Operations Cyber Systems .....	56
Introduction .....	56
Transportation Operations Cyber Systems .....	56
IT Systems used in Transportation Infrastructure Operations .....	58
Industrial Control Systems used in Transportation Operations.....	59
Differences between IT and ICS Cybersecurity .....	61
Highways Operational Systems .....	66
Transit Operational Systems.....	69
Surface Transportation Cybersecurity Issues .....	75
Emerging Trends in Transportation Control Technologies .....	75
Transportation Roadmap for Cybersecurity.....	80
Chapter 5 Countermeasures: Protection of Operational Systems.....	81
Cyber Hygiene.....	83
Access Control.....	84
Data Security and Information Protection .....	86
Boundary Defense and Network Separation .....	88
Configuration Management.....	91

Bring Your Own Device (BYOD) Recommended Security Practices .....	92
Monitoring and Detection .....	94
Chapter 6 Training: Building a Culture of Cybersecurity .....	98
What is a Culture of Cybersecurity?.....	98
Importance of Awareness and Training .....	99
Organizational Support.....	100
Building upon Safety and Security Cultures .....	100
Cybersecurity Awareness and Training Program .....	101
Functions and User Categories .....	104
Content .....	106
Awareness and Training Delivery .....	109
Evaluation.....	111
Performance Indicators.....	113
Continuous Improvement .....	113
Awareness and Training Resources.....	113
Chapter 7 Security Programs and Support Frameworks .....	118
Cybersecurity and Critical Infrastructure .....	118
Control System Cybersecurity Strategy and Roadmaps .....	119
National and Regional Support Resources .....	121
Appendices .....	127

## Tables

Table 1: APTA Cybersecurity Zones.....	49
Table 2: Transportation Operations Systems.....	60
Table 3: IT vs. ICS Security Concept Value.....	61
Table 4: Differences Between IT vs. ICS.....	63
Table 5: : IT vs. ICS Cybersecurity Aspects.....	65
Table 6: ICS Administrative Level Results.....	96
Table 7: Cybersecurity Functions, Elements and Categories.....	107
Table 8: Sample Training Knowledge and Skills.....	109
Table 9: Awareness and Training Subcategories and References.....	117

## Figures

Figure 1: Risk Management Program for Control System Security.....	8
Figure 2: Risk Management/Risk Mitigation Strategies.....	9
Figure 3: Risk Scenario Based Process.....	10
Figure 4: Transportation Information Ecosystem.....	34
Figure 5: Transportation Enterprise Information Systems.....	34
Figure 6: Cybersecurity Risk-Based Framework.....	43
Figure 7: NIST Framework Implementation Steps.....	44
Figure 8: Example of ITD NIST Framework Quarterly Goal Tracking.....	46
Figure 9: Cyber Defense-in-Depth Strategic Framework.....	47
Figure 10: Model Control & Communications System Categories.....	50
Figure 11: Model Transit System.....	51
Figure 12: National ITS Architecture 7.1 - Transportation Layer+.....	67
Figure 13: ITS Security Architecture.....	67
Figure 14: Metrolink’s Positive Train Control.....	72
Figure 15: : Security Credential Management System (SCMS) Functionality.....	77
Figure 16: : Summary of Critical Controls Best Practices.....	82
Figure 17: Typical Transportation System Network with Countermeasures.....	90
Figure 18: Typical Transportation System Network without Countermeasures.....	90
Figure 19: CSET Four Step Process.....	96
Figure 20: MARTA Cybersecurity High-Level Timeline.....	97
Figure 21: Cybersecurity Learning Continuum.....	102
Figure 22: Sample Training Module.....	108
Figure 23: Sample Awareness Posters.....	115
Figure 24: Sample Awareness and Training Program Template.....	116

## Preface

Over the past 40 years we have witnessed a never-ending, escalating evolutionary competition between legitimate developers and users of systems that employ cyber technology and those who seek to do harm. Each generation of cybersecurity solutions is countered by ever-more sophisticated threats; each potential threat spawns additional layers of defense. This Darwinian struggle takes place around the clock and around the globe, involving many thousands of adversaries targeting millions of cyber-components. And unfortunately, the future guarantees more of the same: Cyber defenders and attackers continue their complex “survival-of-the fittest” battle while the rest of nation’s noncombatants bear its ever increasing consequences.

During much of this time, surface transportation owners, transit operators, motorists and riders were relatively insulated from this arena. Vehicles were “dumb,” roads were even dumber and save for the occasional embarrassment over roadside message signs being hacked, neither transportation engineers nor the traveling public were aware of or concerned with the need for cybersecurity, particularly as it related to the operations of the transportation highway and transit infrastructure.

The emergence of Intelligent Transportation Systems (ITS) did little to change things: transit vehicles got smarter, the first generation of digital roadside devices and systems were stand-alone solutions with advisory responsibility only (e.g., variable message signs, road weather systems) and the few technologies that had safety ramifications such as traffic signal controllers remained isolated and difficult to access. Minimal attack exposures coupled with negligible consequences to human safety translated to low risk. Consequently, policy makers and program managers were unconcerned about threats to their investments, their services and their customers. Indeed, during most of this time, there were very few (reported) cybersecurity breaches involving transportation system operations, reinforcing the sector’s complacency.

In recent years cloud or network computing has revolutionized every sector of the economy, including transportation; the cloud is now ubiquitous, mobile and hyper-connected. Unsurprisingly, manufacturers of infrastructure control systems thrived in this new environment. Control system components and networks are now accessible from anywhere and are increasingly connected to enterprise data, customer satisfaction and entertainment networks. Analog controls are being replaced by networked digital counterparts, allowing remote monitoring and control of signals, signs, bridges, tunnels and vehicles – public and private. Although core functionality has greatly increased due to this new connectivity, so also has the exposure to multiple threats coming from local and distant sources.

The sheer numbers of suddenly visible, interconnected, increasingly vital cyber components now deployed in transportation system and transit operations have created enormous, underappreciated complexity and significantly greater vulnerability across the entire system. Not only are single components at greater risk, but the cascading effects caused by intentional cyber-attacks and also by non-malicious incidents (e.g., component failure, network failure) should give even the most conservative transportation engineer pause. As one cybersecurity expert put it, “Unintentional impact doesn’t mean insignificant impact.” This

situation is poorly understood by transportation system executives, program managers, employees, elected officials and regulators.

Paradoxically, the relatively few numbers of catastrophic incidents to date has resulted in a false sense of security within the transportation sector, although it should be kept in mind that few agencies are interested in revealing security breaches and their impacts. Recent work conducted by this research team estimated that as many as 75% of physical security breaches go unreported. The research team has no reason to believe that this estimate is any lower for cyber incidents.

The research Team appreciates the difficulty that this situation presents agencies, regulators and elected officials: how can the reassignment of scarce resources to cybersecurity be justified in the absence of a clear and present danger, the pressure of competing priorities with larger constituencies, the complexity of the situation and the confusion resulting from overlapping, splintered responsibility for the situation.

In short, transportation managers and employees are wrestling with a novel situation, with little understanding of the contours of the challenge, the parameters of the response or the seriousness of the consequences. As a former Secretary of Defense put it, *“There are known knowns; there are things we know that we know. There are known unknowns; that is to say there are things that we now know we don't know. But there are also unknown unknowns – there are things we do not know we don't know.”* Many, if not most aspects of cybersecurity across the transportation sector can fairly be characterized as unknown-unknowns at this point.

This “Cybersecurity 101” Primer provides transportation organizations basic reference material concerning cybersecurity concepts, guidelines, definitions and standards. The Primer delivers fundamental strategic, management and planning information associated with cybersecurity and its applicability to transit and state DOT operations. The Primer presents fundamental definitions and rationales that describe the principles and practices that enable effective cybersecurity risk management.

This Primer aims for concrete and measurable goals: increase awareness of cybersecurity as it applies to highway and public transportation, plant the seeds of organizational culture change, address those situations where the greatest risks lie, and provide industry-specific approaches to monitoring, responding to and mitigating cyber threats. This reference guide seeks to bridge a known knowledge gap by providing transportation managers and employees with greater context and information regarding the principles of information technology and operations systems security planning and procedures.

## Organization of the Primer

This Primer contains seven Chapters discussing various dimensions of transportation cybersecurity and provides numerous references, case studies and examples throughout. With the exception of domain-specific systems discussed in Chapter 4, the material is intended to be of equal interest in highway infrastructure and public transportation settings. Each Chapter provides basic and general information for the novice cybersecurity manager and includes a



rich set of resource references more suitable for the seasoned security professional.

**Chapter 1 Top Myths of Transportation Cybersecurity.** Chapter 1 rebuts common misunderstandings that may be impeding enterprise action on cybersecurity.

**Chapter 2 Cybersecurity Risk Management, Risk Assessment and Asset Evaluation.** Chapter 2 presents a systems approach to risk management and discusses various strategies and resources used in Risk Management, Risk Assessment and Asset Evaluation, Threat Assessment, Vulnerability Assessment and Consequence or Impact Assessment

**Chapter 3 Cybersecurity Plans and Strategies, Establishing Priorities, Organizing Roles and Responsibilities.** Chapter 3 presents enterprise-wide approaches to cybersecurity enhancement and governance strategies and includes discussions on security planning, American Public Transit Association's (APTA) recommended security program, establishing priorities, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, a general overview of "Defense in Depth" cybersecurity and "security zones" approaches, attack modeling, organizing roles and responsibilities, relationship with physical security and vendor approaches from a transportation perspective.

**Chapter 4 Transportation Operations Cyber Systems.** Chapter 4 discusses the difference between data and control systems and provides overview of each of these in both the highway infrastructure and public transit domains. The Chapter also discusses emerging trends in transportation systems including connected and automated vehicle technologies.

**Chapter 5 Countermeasures: Protection of Operational Systems.** Chapter 5 presents the basics of cybersecurity and discusses best practices in the areas of cyber hygiene, access control, data security and information protection, boundary defense and network separation, configuration management and Bring Your Own Device (BYOD), system monitoring and intrusion detection.

**Chapter 6 Training: Building a Culture of Cybersecurity.** Chapter 6 discusses the behavioral, cultural, organizational and institutional aspects of cybersecurity and presents a framework for building effective awareness and training programs and follow-up performance evaluations.

**Chapter 7 Security Programs and Support Frameworks.** Chapter 7 introduces National and Federal policies, regulations, frameworks, tools and other resources useful in setting up a comprehensive cybersecurity function that is consistent, coordinated and compatible with activities at other agencies and in other Sectors.

## Executive Summary

Protecting transportation systems from adverse events that would compromise the delivery of services to the passengers and shippers who depend upon them includes eliminating or minimizing the risk and exposure to harm resultant from hazards, accidents, or physical or cyber attacks against critical assets or mission essential activities and resources. Today, transportation agency leadership, management and staff face even greater levels of risk and exposure to these types of events than ever before.

In the context of cybersecurity the sheer numbers of interconnected, increasingly vital cyber components now deployed in transportation systems and transit operations has created significantly greater vulnerabilities across systems and networks. Not only are single components at greater risk; the cascading effects caused by both non-malicious incidents (e.g., accidents, component failure, network failure) and also intentional cyber-attacks has created a modern day transportation operating environment that warrants the full attention of senior management and the commitment of significant agency resources to effectively maintain mission critical functions.

Consequences of cyber incidents differ widely in their impact, duration, and cost. Events causing catastrophic loss of life or enterprise threatening economic damages remain rare, however they are increasing in frequency. Lesser events that result in actual or perceived risk of harm or increased liability, potential compromise of the safety and security of passengers or employees, short-term financial losses, or that compromise the reputation and goodwill of the agency can occur at any time. Cyber risk also does not exclude smaller or less complex systems. While the scope and comparative impact of an incident at a medium or smaller sized agency may be lessened in severity there is still a potential for the loss of assets and functionality that can disrupt the delivery of essential services or cripple agency operations. There have already been instances of unsafe, curtailed or disrupted service, loss or theft of personal or proprietary data, increased litigation exposure or cost, or unacceptable compromise of customer expectations. And from the standpoint of consequence it does not matter if the harm was deliberately caused.

Paradoxically, the relatively few numbers of catastrophic incidents in transportation to date has resulted in a false sense of security within the transportation sector. Recent research estimated that on the physical security side as many as 75% of security breaches go unreported. In terms of cyber much less is known about prospective breach percentages, but there is little reason to believe that the numbers are any better for cyber incidents. What is known is that the ease of compromise of transportation cyber systems is becoming more and more evident, and the likelihood of new or more significant events is increasing along with the per event costs of cyber incidents and cyber-crime.

A good working definition of cybersecurity for transportation is one put forth by ISA/IEC-62443 (formerly ISA-99), a baseline security standard for industrial control systems, that defines cybersecurity more broadly as “electronic security” whose compromise could result in any or all of the following situations:

- Endangerment of public or employee safety

- Loss of public confidence
- Violation of regulatory requirements
- Loss of proprietary or confidential information
- Economic loss
- Impact on national security

There are common myths about cybersecurity and transportation systems that are creating misunderstanding. Dispelling these myths will allow transportation agencies to more efficiently and effectively improve the cybersecurity and resilience of critical transportation infrastructure. There are approaches to reduce transportation cybersecurity risks and mitigate the impacts of cyber incidents.

#### **Common Cybersecurity Myths**

Nobody wants to attack us.  
 It can't happen to us.  
 It's all about IT.  
 It's possible to eliminate all vulnerabilities.  
 Cybersecurity incidents will not impact operations.  
 Control system and IT cybersecurity are same.  
 Cybersecurity needs to be solved only once.

Managing the risks associated with cyber for IT and ICS can prove to be intractably challenging. For transportation agencies the response to the challenge lies in the formulation of a program that both balances and shares responsibility for critical infrastructure system protection among operators and employees, government agencies, industry stakeholders, technology manufacturers and product vendors. The NIST Cybersecurity Framework provides guidance that transportation agencies can utilize.

Unlike physical security protection systems where countermeasures can be deployed by an organization to harden a critical asset, “locking down” cyber systems demands that vulnerabilities be identified and eliminated, reduced or mitigated along the entire technological supply chain. Overcoming the global threat posed by international attackers who can exploit from afar adds a dimension to the problem that requires participation by government, and by extension, the entire international community. In addition, cybersecurity is a continual process with evaluation and monitoring as key components to identify and manage changes to systems and environments.

Security planning directs a transportation agency towards prevention and mitigation of the effects of security incidents by integrating those approaches that have proven to be successful into the operating environment. Development of a security plan provides an effective means to meet cost-benefit and competitive resource challenges. Cybersecurity planning should incorporate, at the minimum:

- Security strategy that expresses management's commitment to cybersecurity and provides the high-level direction and requirements for cybersecurity in the agency.
- Security policies that address the range of management, personnel, operational and technical issues and guide the development, implementation and enforcement of the agency security measures.

- Roles and responsibilities that clarify decision- making authority and responsibility for cybersecurity.
- Vulnerability and risk assessments to identify the agency-specific security requirements and assist in prioritization of risk management efforts. Although there are variations in application, the risk management process for transportation agencies in this cyber environment requires consideration and adoption of many of the same security principles used in the protection of physical assets.
- Development and Maintenance of cybersecurity plans including Risk Mitigation/ Management and Response/Recovery plans.
- Active monitoring and evaluation on a continuous basis.
- Awareness and Training for all agency employees.

#### APTA Recommended Security Plan Elements

##### Control/Communications systems boundaries

- Identify the systems.
- Identify the equipment.
- Identify the locations.
- Identify the stakeholders.

##### Work group

- Include all stakeholders.
- Identify responsibilities.

##### Policies and procedures

- Administrative
- Technical
- Cyber
- Physical
- Maintenance

##### Security measures

- Management reports
- Maintenance issues
- Training

When planning for cybersecurity, some principles should be kept in mind:

**Address cybersecurity planning in a systematic way**, with a commitment to a process of continuous improvement. Even with unlimited resources, it is not possible to eliminate all vulnerabilities and risks.

**Take a balanced approach** that focuses on standards and incorporates learning from experience. Any cybersecurity program should be approached using risk management practices as a guide. Evaluate the agency's specific cyber risks and develop the cybersecurity plan around managing those risks.

**Security policy and controls must be adaptable** to emerging threats in a constantly evolving world. Vulnerabilities are evolving and new risks are growing by the hour. Maintain situational awareness of cyber threats – both intentional and unintentional as part of the plan.

**Failure will happen** so it is important to plan for it, isolate it, contain its damage and recover from it gracefully. It is important to recognize that perfect security is not possible and that everything cannot be mastered. Planning ahead – having a Cyber Response and Recovery Plan - can ensure less damage from an incident.

Guidance exists for general cybersecurity plans. To date no comprehensive guidance has been developed to provide support for a transportation agency cybersecurity plan, although APTA has provided a recommended practice that includes security plan elements. The Roadmap to Secure Control Systems in the Transportation Sector (DHS, 2012) was developed to assist transportation

agencies develop plans and the culture needed to sustain those plans. Guidance tailored for other sectors (e.g. nuclear, electrical and water) also has relevance for the transportation sector.

Other types of plans that support cybersecurity resiliency include:

- **Incident Response Plan** which addresses the ability to proactively detect, contain, eradicate and recover from a cyber incident. As part of the response plan it is important to be prepared to isolate systems and to preserve forensic evidence for analysis. The robustness of a transit agency's incident response will vary depending on its budget, size and capability. However, smaller transit agencies can implement basic practices and work with other agencies to foster information sharing. All transit agencies should have some form of incident response.
- **Business Continuity Plan (BCP)** that focuses on sustaining an organization's mission/business processes during and after a disruption, written for a single business unit or the entire organization's processes. The Plan can be scoped to address only priority functions. Because mission/business processes use information systems, the business continuity planner must coordinate with information system owners to ensure that the BCP expectations and information system capabilities are matched.
- **Continuity of Operations Plan (COOP)** which focuses on restoring an organization's mission-essential functions and performing those functions for up to 30 days before returning to normal operations. Additional functions may be addressed by the Business Continuity Plan.
- **Crisis Communications Plan** that provides standard procedures for internal and external communications in the event of a disruption should be documented using a crisis communication plan. The plan provides various formats for communications appropriate to the incident and designates specific individuals as the only authority for answering questions from or who provide information regarding the response. The plan may also include procedures for disseminating reports to agency personnel on the status of the.
- **Disaster Recovery Plan (DRP)** that typically applies to major disruptions to service and is designed to restore operability of the system, application or cyber infrastructure after an emergency. A DRP may support a Business Continuity Plan or a COOP.

There is a rich body of cybersecurity guidance and resources from an IT perspective that has developed over the past 40 or so years. There is a growing body of cybersecurity guidance and resources developing today for control system cybersecurity. Practices and countermeasures that are "best practices" from both these perspectives. The Cybersecurity Guide identifies effective practices that can be used to protect transportation systems from cyber events and to mitigate damage should an incident or breach occur. Those practices include cyber hygiene, access control, data security and information protection, boundary defense and network separation, configuration management, and monitoring/detection.

The Guide is designed for all surface transportation - both transit and highway - agencies and is intended to cover all transportation systems - industrial control, transportation control, communications and enterprise data systems. However, a special focus has been placed on systems associated with the control of transportation infrastructure assets. This approach is a recognition that viewing cybersecurity from an IT perspective alone is proving to be both short-sighted and of limited effectiveness.

## Introduction

Today's "cyber" transportation systems consist of a convergence of operating control systems and information technology networks that are blended together to enable the delivery of mission critical services to the travelling public, shippers, and other users. This convergence has created a unique set of expanding opportunities for the transportation industry to deliver top quality services; but simultaneously a new downside risk vector has evolved that threatens the functionality of transportation systems and the people who have come to rely upon them. In the past, transportation systems were closed proprietary systems. Protected by "air gaps" and "security by obscurity" they had very limited cyber vulnerabilities compared to IT networks and systems. Over time there has been a shift from isolated systems to more connected systems. Proprietary applications have migrated to open protocols, inheriting vulnerabilities along the way. Remote sites and stand-alone systems are accessed through wireless and public or private networks. Formerly "closed" systems are integrated and shared or there are in-place joint-use systems for the enterprise with linkages to transportation network systems.

In addition to customary concerns about the physical security of transportation systems now information and control system security has been brought to the forefront. Indeed the risk of harm, including the potential for significant loss of life to the public, intolerable financial burden or bankruptcy, or long-term damage to business reputation that is associated with the movement of people and goods has grown substantially through an increased reliance by transportation operators upon sophisticated interconnected information networks and technologies that are used to control and influence the performance of transportation's critical infrastructure.

The "cyber" threat vector is now becoming known. Well publicized incidents in finance and banking, and perhaps most frequently the retail sector have elevated public awareness of the potential for serious injury, mostly financial injury, through the intentional exploitation or disruption of information networks.

However the added dimensions of cyber risk now associated with operating control systems that go well beyond financial concerns are not as well understood. And transportation industry leaders because of the nature of their services, must take accountability for downside cyber risk and prioritize their thinking to increase preparedness and reduce cyber vulnerabilities. Transportation, energy, water, and banking all represent a combination of public and private interdependent systems that are exploitable by intentional cyber-attacks or susceptible to accidental compromise. There is an immediate need for those responsible managers and operators in these industries to engage in risk assessments and planning for the security of cyber control systems. All transportation systems today rely on both physical and cyber systems to support mission critical services. And even these physical and cyber aspects of transportation are converging at an accelerating pace.

Fortunately neither the occurrence of accidents nor the exploitation of transportation industry cyber assets has resulted in the types of events that grab national headlines. However the ease of compromise of transportation systems is becoming more and

more evident. And the likelihood of new or more significant events is increasing along with the cost of cyber incidents and cyber-crime:

- In 2006, two employees hacked into the traffic control computer in Los Angeles as part of a labor dispute and demonstrated how easily a major city could become gridlocked. Choosing locations they knew would cause significant backups, e.g. close to freeway entrances and major destinations such as airports, the engineers caused major traffic congestion that took four days to completely resolve. Although no reported accidents or injuries were associated with the incident, the full impact was significant with delays and potential inabilities of emergency vehicles to get to their destinations and loss of economic productivity as people were stuck in their cars.
- In 2008, a Polish teenager proved that even proprietary closed systems are vulnerable by using a modified a TV remote to control the track switches of the Tram system. The resulting derailment fortunately did not cause any loss of life, but 12 passengers were injured in the incident.
- In 2009, a computer crash in Maryland showed that unintentional and accidental events can have serious consequences. The crash caused the loss of traffic signal controls and power failures in the system, resulting in significant delays for thousands of commuters.
- In 2009, the hack of smart parking meter introduced transportation agencies to the new world of cybercrime, where incidents are now being planned and targeted so as to acquire significant profits. The impact for the transportation agency can now include significant revenue loss along reputational and mission-related consequences.
- In 2011, the politically active hacker group, Anonymous, took aim at transportation to protest a transit agency's policies. The group defaced the BART public information website to make their presence known and collected agency customer's personally identifiable information from the agency's data systems to use to be used as a weapon to obtain concessions from BART. Anonymous threatened to release the customer information.
- In recent years, dynamic message signs have been a frequent target for hackers, changing them to display humorous and sometimes obscene messages. Fortunately none of these incidents resulted in more than mischief. The potential for more serious consequences such as traffic accidents did not occur. In 2014, the stakes were raised when multiple signs in different locations were changed at the same time by a hacker, demonstrating the ability to do more serious damage. FHWA and US Computer Emergency Response Team (CERT) quickly worked to understand the incident and contain the risk in the future.

**Average Cost of Cyber Incidents in U.S.**

*Average cost of cybercrime: \$12.7 million.*

*Average cost of data breach: \$3.5 million based average cost of \$145/record.*

*Transportation industry cost per record is \$121/record.*

*Source: 2014 Cost of Data Breach Study: Global Analysis, Ponemon study*

A good working definition of cybersecurity for transportation is one put forth by ISA/IEC-62443 (formerly ISA-99), a baseline security standard for industrial control systems (ICS). It

defines cybersecurity more broadly as “electronic security” whose compromise could result in any or all of the following situations:

- Endangerment of public or employee safety
- Loss of public confidence
- Violation of regulatory requirements
- Loss of proprietary or confidential information
- Economic loss
- Impact on national security

As previously mentioned unintentional incidents should be of equal concern to transportation leaders. From the standpoint of consequence or end result it usually matters not whether a harm was deliberately caused. And typically structural network failures and human errors have the potential to occur more frequently than intentional cyber-attacks.

The objective of this Cybersecurity Guide is to identify effective practices that can be used to protect transportation systems from cyber events and to mitigate damage should an incident or breach occur. There is a rich body of cybersecurity guidance and resources from an IT perspective that has developed over the past 40 or so years. There is a growing body of cybersecurity guidance and resources developing today for control system cybersecurity. The Guide will highlight cybersecurity practices and countermeasures that are “best practices” from both these perspectives.

The Guide is designed for all surface transportation - both transit and highway - agencies and is intended to cover all transportation systems - industrial control, transportation control, communications and enterprise data systems. However, a special focus has been placed on systems associated with the control of transportation infrastructure assets. This approach is a recognition that viewing cybersecurity from an IT perspective alone is proving to be both short-sighted and of limited effectiveness.

Because technology is rapidly evolving, cybersecurity involves addressing a rapidly changing set of vulnerabilities and risks. Today, transportation agencies today are wrestling with approaches to handle use of mobile, tablet and other small hand-held devices in the systems. The ramifications of driverless and other connected vehicles are currently being explored. The Internet of Things is already here and changing every day. The Guide was developed with a forward looking with an eye towards what risk related exposures appear on the landscape for the industry. Forward looking cybersecurity guidance and resources must also include a focus upon the interface and inclusion of critical infrastructure operating systems with other facilitative information technology processes and systems.

In summary, the Cybersecurity Guide aims for implementable goals: to increase awareness of cybersecurity in transportation agencies; to support an operational, as opposed to a technical, approach to cybersecurity; to identify those situations where the greatest cyber risk lies; and to provide transportation-specific approaches to monitoring, responding to and mitigating cyber threats.



## Chapter 1 Top Myths of Transportation Cybersecurity

If common myths about cybersecurity and transportation systems are understood and misunderstandings are dispelled, then transportation agencies can more efficiently and effectively improve the cybersecurity and resilience of critical transportation infrastructure.

1. **“Nobody wants to attack us.”** Other sectors are more likely targets for cyber-incidents than transportation, it won’t happen in transportation.

Transportation systems are vulnerable to the same and/or similar cyber risks as other industries that use industrial control networks and information systems to accomplish their core business functions. Cyber-incidents have occurred in transportation systems and reported instances are growing. In 2013 the security camera apparatus in the Israeli Carmel Tunnels was affected, shutting down the toll road over two days causing major traffic congestion and disruption. Eleven percent of control system incidents reported to Industrial Control Systems (ICS)-CERT in 2012 were in the transportation sector, a number that has been growing over time.

Cybersecurity incidents are not always intentional attacks on specific systems such as the 2011 BART website assault by the hacker advocacy group “Anonymous” to protest the transit agency’s temporary shutdown of underground cell phone service. Because cyber-intruders want to use unsuspecting systems to attack others or to send bulk email, they conduct network searches to find vulnerable systems and identify any useful resources on the networks found. These “probes” can have significant consequences due to inherent vulnerabilities in control systems within transportation systems. In addition, cybercrime is expanding. Modern cybercrime operations are sophisticated, well-funded, and capable of causing major disruption to organizations. Cybercriminals usually have clear business objectives - they know what information they are seeking and they plan to profit from it. Transportation systems are attractive to cybercriminals. Smart parking meters were first hacked in 2009. Transit fare cards have been an ongoing target since then.

Some incidents may not have been recognized as “hacking” and so are not thought of as a cybersecurity issue. In 2006 a disgruntled employee hacked into a traffic control computer in Los Angeles and shut down signals at key points causing delays for four days. Equipment failures or even maintenance procedures can cause unexpected incidents such as a loss of traffic management capabilities or signaling systems.

Because of the increasing dependence on connected systems and networks with inherent vulnerabilities (control systems, fare/payment systems, wireless systems, mobile and smart devices), expanding opportunities for cyber incidents (positive train control, ITS, V2V, V2I), and the unique challenges from connectivity of safety-critical control systems such as those found in vehicles and in highway Advanced Traffic Management Systems, cyber risks are significant and growing in transportation.

2. **“It can’t happen to us”**. Our systems are “air gapped” or “firewalled”.

In the past, transportation systems were closed proprietary systems that were protected by “air gaps” and “security by obscurity” with limited cyber vulnerabilities. The 2008 derailment of a Polish Tram by a 14-year-old boy using a TV Remote Control unit to manipulate the transit system switches demonstrated that even then an “air gap” was not enough. Today, the proprietary applications have migrated to open protocols, inheriting vulnerabilities along the way. Remote sites and stand-alone systems are accessed through wireless and public or private networks. For example, remote access for support and maintenance personnel or maintenance laptops connected directly to control systems, bypassing firewalls and policy rules, is not uncommon. Often, the system owner has no knowledge of the systems being used for maintenance, or the personnel using the systems in these ways. Systems are integrated and shared or joint-use enterprise systems with linkages to transportation network systems for management and financial reporting (and sometimes e-commerce) open up “closed” systems. Although systems are closed, there may be open connections that are not discovered as systems become integrated.

Assuming that the firewall is correctly configured (rules complexity and the specifics of the control systems in place have to be taken into account), a firewall cannot protect against insiders, filter the content of encrypted connections, or protect against connections that do not go through it. In today’s environment of sophisticated hacker tools and easily available shared techniques that are constantly evolving, firewalls are not enough. Adversaries are developing new methods for embedding malware in networks, remaining undetected for long periods, and stealing data or disrupting critical systems.

3. **“It’s all about IT”**. Most of the cybersecurity investment will be in technology.

Having technology in place to provide cybersecurity is only one part of effective cybersecurity. People and processes are just as important as technology in improving cybersecurity. Agency personnel need to be aware users of the systems in place: aware of the risks to the systems and to themselves. People are vulnerable to manipulation and social engineering that results in providing confidential information through phishing emails or conversations with strangers. People need to be aware of security policies and procedures that have been put in place. Management must actively support the cybersecurity program in a visible manner. A process tied to the security strategy with policies and procedures to support strategy is critical to establish an agency-wide culture of security. ***APTA Recommended Practices Securing Control and Communications Systems in Rail Transit Environment, Part 2*** recognize the importance of a cybersecurity culture in the agency.

*Just as transit agencies have created a safety-centric culture—saving lives and reducing accidents and accident severity—they need to foster and create a cybersecurity culture. This requires an awareness program; a training program; an assessment of cybersecurity threats; a reduction of the attack surface (the number of places and ways someone can attack transit systems); a cybersecurity program that addresses: threats, mitigations, the software/firmware update process, monitoring and detection methodologies; and the ability to be audited to check for compliance via logs*

*and change-management systems.*

4. **“It’s possible to eliminate all vulnerabilities in systems”.** Cybersecurity incidents can be completely prevented.

The *DHS National Cybersecurity Division Common Vulnerabilities and Exposures* (CVE) list has more than 50,000 recorded vulnerabilities -- with more added hourly. There are 86,000 new pieces of malware reported each day. The odds are high that your transportation systems have already been infiltrated. According to a recent Cisco Security Report, all of the organizations Cisco examined during 2013 showed evidence of suspicious traffic, evidence that these networks have been penetrated.

Due to the complexity of today’s transportation systems and human fallibility, perfect security is impossible to achieve. A more effective strategy is to assume that a cybersecurity incident will happen and focus on mitigating the consequences.

#### 5. **“Cybersecurity incidents will not impact operations.”**

A 2005 Report by the National Institute for Advanced Transportation Technology that assessed the security of transportation control networks (*Assessing the Security and Survivability of Transportation Control Networks, P. Oman, 2005*) found that control center and dispatch communications, equipment for access, safety and monitoring, and real-time actuators regulating transportation flow (e.g., bridges, tunnels, rail crossings, arterial routes, etc.) were at risk. Especially vulnerable were in-the-field devices used to monitor and regulate traffic flows in large urban environments. Since that time some improvements in security have been made but operational systems are still vulnerable.

Stuxnet, discovered in June 2010, was the first known instance of cyber sabotage to real world operational systems as opposed to disruption of IT systems. Different from anything seen before, the cyber worm targeted control systems with the intention to reprogram control system components in a manner that would sabotage operations, hiding the changes from programmers or users.

#### 6. **“Control system cybersecurity can be handled the same as IT cybersecurity.”**

Adding cybersecurity components to transportation control systems requires personnel that understand security components and also the controls systems and the operational environments that they control. Securing access to and control of the network is generally the responsibility of information technology (IT) personnel. Control systems are usually the responsibility of the engineering and operations personnel. There are differences between IT systems and control systems that need to be recognized. *NIST Special Publication 800-82 Guide to Industrial Control Systems Security (2011)* summarizes some of the differences:

*Although some characteristics are similar, ICS also have characteristics that differ from traditional information processing systems. Many of these differences stem from*

*the fact that logic executing in ICS has a direct effect on the physical world. Some of these characteristics include significant risk to the health and safety of human lives and serious damage to the environment, as well as serious financial issues such as production losses, negative impact to a nation's economy, and compromise of proprietary information. ICS have unique performance and reliability requirements and often use operating systems and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of control systems.*

Special precautions must be taken when introducing security to ICS environments. In some cases, new security solutions are needed that are tailored to the ICS environment.

#### **7. “Security is a problem that needs to be solved only once.”**

Control systems and field devices require active configuration and maintenance. Not only must the systems and devices be secured, their ongoing management and maintenance need to be secured as well, and must be capable of managing changes and adapting to new vulnerabilities or the emergence of new threats. There are approaches to reduce the cybersecurity risks and mitigate the impacts of incidents. In an ever-changing security landscape, cybersecurity must be a continual process with evaluation and monitoring as key components to identify and manage changes to systems and environments.

## Chapter 2 Cybersecurity Risk Management, Risk Assessment and Asset Evaluation

### Risk Management

Managing the risks associated with cyber, IT and ICS, can prove to be intractably challenging. For even the most robust and up-to-date security systems there is an ever-growing risk that the next exploitation methodology will be discovered by an attacker and be introduced without detection. And in truth it takes the commitment of significant resources, and the development of substantial expertise to establish and maintain an effective cybersecurity program or response capability.

For transportation agencies the response to the IT and ICS security challenge lies in the formulation of a program that both balances and shares responsibility for critical infrastructure system protection among operators and employees, government agencies, industry stakeholders, technology manufacturers and product vendors. Unlike physical security protection systems where countermeasures can be deployed by an organization to harden a critical asset, “locking down” cyber systems demands that vulnerabilities be identified and eliminated, reduced or mitigated along the entire technological supply chain. Overcoming the global threat posed by international attackers who can exploit from afar adds a dimension to the problem that requires participation by government, and by extension, the entire international community.

Although there are variations in application, the *risk management* process for transportation agencies in this cyber environment requires consideration and adoption of many of the same security principles used in the protection of physical assets. *Transportation Cyber Risk Management is the process whereby transportation risk scenarios are analyzed and acted upon.* This includes scenarios wherein accidents are deliberately caused, public transportation services are rendered unavailable, carrier systems lose location



**Figure 1: Risk Management Program for Control System Security**  
 Source: PowerPoint Presentation on Control Systems Security Program – Transportation DHS CSSP ICSJWG Conference – Seattle October 27, 2010 | David Sawin Volpe Program Manager, Information Assurance (Control Systems)

The Volpe Center has been supporting the DHS Control System Security Program in Transportation. The Volpe Cybersecurity Life Cycle Support has Risk Management at its core as represented in the above Chart. RM is surrounded by four continuous workflow processes – design, assess, implement and operate. The processes are further broken down into functional areas – security policy, privacy, security architecture, system prioritization, risk assessment, remediation and implementation, security test and evaluation, awareness and security training, and intrusion detection.

identifiers, and shipments are irretrievably lost. Optimally, significant inherent operational risk should be viewed in the context of transportation business and environmental control factors resulting in recommendations for *Risk Response Options*.



**Figure 2: Risk Management/Risk Mitigation Strategies**

Adapted from NCHRP Report 525 Volume 14, Security 101: A Physical Security Primer for Transportation Agencies

*Response Options include Risk - Avoidance, Acceptance, and reduction strategies including Assessment, Dependency and Spreading, and Transfer.*

Avoidance, the simplest of all solutions for eliminating risk consists of refraining from engaging in the risky activity in the first place. For example, in the scenario where cyber risk is presented by a technological automation of an operational system, the alternative of a non-cyber ventilation system will eliminate the cyber related risk of automating fan mechanisms. However, in this rudimentary example it becomes readily apparent that one or more

employees will be required to manually turn on and turn off each and every one of the ventilation systems fans when required in order to make the system function.

Similarly, acceptance of risk requires no real action to be taken by the organization. But acceptance should be based on a knowledgeable and responsible recognition of the probability and impact of perceived adverse cyber events. Because of the increased interface and integration of modern day cyber assets obtaining accurate information for this approach can be somewhat difficult to accomplish. Typically cost-benefit analysis can be utilized to determine the tipping point where expending funds to fix a problem exceeds the return on investment that the mitigation achieves. However with cyber the full measure of probable or likely losses is difficult to identify. Issues’ regarding the potential for loss of life now being more so associated with integrated transportation ICS systems further exacerbates the problem.

However, most cyber risk is dealt with using *Risk Reduction* techniques. Identifying and eliminating the *vulnerabilities* of IT and ICS systems is clearly the main method of reducing or mitigating losses. Vulnerabilities are identified, catalogued, shared and “patched” a process that is essential to the response methodology of cybersecurity professionals. Non-professionals are taught IT systems “awareness” as a means to minimize human interface (HMI) types of vulnerabilities from breaching IT or ICS. Of note, it is estimated that between 300,000 & 1M current cybersecurity positions are vacant. Demand is expected to rise as public, private

and government sectors face unprecedented numbers of data breaches and cybersecurity threats.

Today the lack of cybersecurity talent can be an organization's biggest vulnerability, exposing it to serious risk that can equate to unacceptable losses.

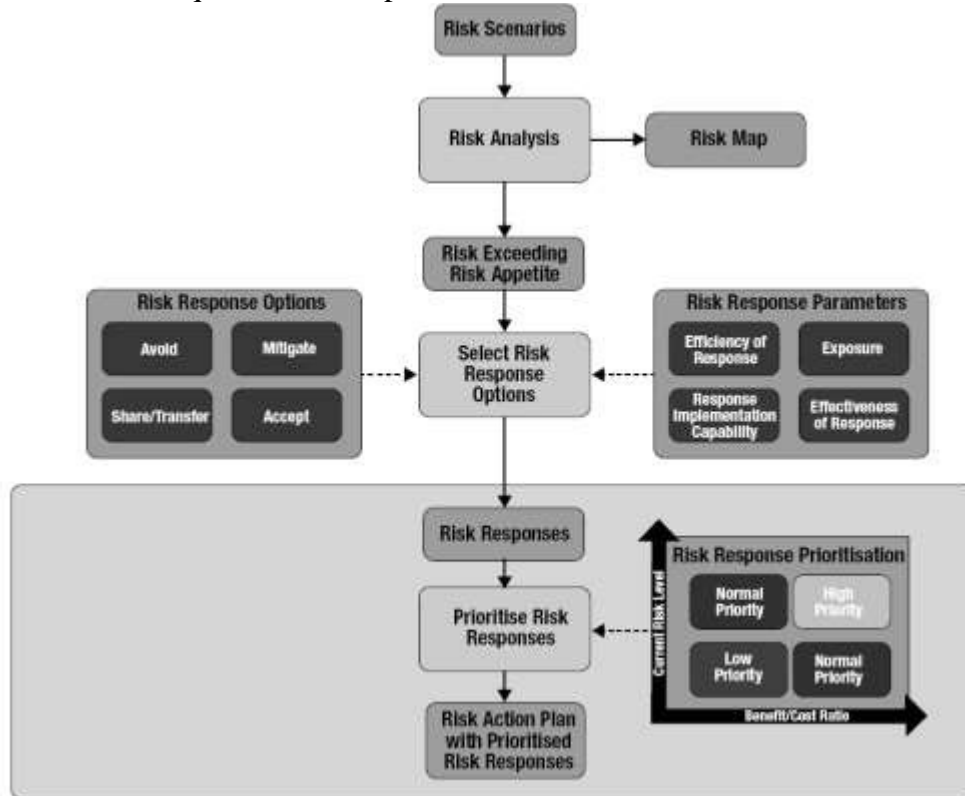


Figure 3: Risk Scenario Based Process

Adapted from COBIT 5 for Risk, the Information Systems Audit and Control Association – [www.isaca.com](http://www.isaca.com)

In addition to managing risk through vulnerability analysis, other reduction techniques can be deployed. *Risk Dependency and Spreading* takes into account that coordinated collaboration amongst cybersecurity stakeholders including end user operators, information security practitioners, designers, manufacturers and distributors, integrators, standards organizations and government regulators can result in the identification of defensive strategies to effectively reduce cyber risk. Maximizing the accountability of all stakeholders in the supply chain presents the opportunity for a strong and systematized approach to managing risk that is both highly efficient and cost effective.

Best illustrated through discussion of control systems, the spreading of risk in terms of cyber takes into account that historically control system security was a function of total isolation from external networks. Operations commands, instruction and data acquisition occurred in a closed environment. But today's systems are very different. There are now integrated architectures that connect external sources: the corporate LAN, peer sites, business partners and vendors, remote operations and facilities and the Internet. Protecting what was formerly an isolated ICS system, with little if any cybersecurity defenses can be extremely

challenging. Particularly since the very nature of an open architecture network demands the exchange of data from disparate information sources, of which an attacker could take advantage. Risk spreading recognizes that all parties or providers to the integrated network architecture, including vendors, suppliers, business partners, corporate, security departments and the government, share responsibility to deploy mitigation strategies and countermeasures that will reduce the vulnerabilities of the system.

*Risk Transfer*, the use of insurance to transfer all or parts of liability to another business or entity, is one of the traditional market mechanisms for estimating, pricing, and distributing risk. According to the International Risk Management Institute's Annual Survey of specialized insurance services, businesses spent as much as 2B on cyber insurance premiums in 2013. Some estimates suggest that the number has jumped to 5B in 2014. Cybersecurity is one of the fastest growing lines of insurance. Particularly for companies that hold customer personal data or even employee data for companies with large numbers of positions and staff – credit card numbers, medical information, social security numbers, coverage can cost more.

## Risk Assessment and Asset Evaluation

A mainstay of both physical and cyber systems security, risk reduction consists primarily of the assessment of threats, vulnerabilities and consequences (TVC analysis) of an event or series of events in an effort to reduce or mitigate losses associated with their occurrence. Risk assessments address the potential adverse impacts to organizational operations and assets, individuals, other organizations, and the economic and national security interests of the United States, arising from the operation and use of information systems and the information processed, stored, and transmitted by those systems. Organizations conduct risk assessments to determine risks that are common to the organization's core missions/business functions, mission/business processes, mission/business segments, common infrastructure/support services, or information systems.

***NIST Special Publication 800-30*** summarizes the steps associated with risk assessment as follows:

### ***STEP 1: PREPARE FOR RISK ASSESSMENT***

Task 1-1. **Identify Purpose** – Identify the purpose of the risk assessment in terms of the information that the assessment is intended to produce and the decisions the assessment is intended to support.

Task 1-2. **Identify Scope** – Identify the scope of the risk assessment in terms of organizational applicability, time frame supported, and architectural/technology considerations.

Task 1-3. **Identify Assumptions and Constraints** – Identify the specific assumptions and constraints under which the risk assessment is conducted.

Task 1-4. **Identify Information Sources** – Identify the sources of descriptive, threat, vulnerability, and impact information to be used in the risk assessment.

Task 1-5. **Identify Risk Model and Analytic Approach** – Identify the risk model and analytic approach to be used in the risk assessment.



*STEP 2: CONDUCT RISK ASSESSMENT*

Task 2-1. **Identify Threat Sources** – Identify and characterize threat sources of concern, including capability, intent, and targeting characteristics for adversarial threats and range of effects for non-adversarial threats.

Task 2-2. **Identify Threat Events** – Identify potential threat events, relevance of the events, and the threat sources that could initiate the events.

Task 2-3. **Identify Vulnerabilities and Predisposing Conditions** – Identify vulnerabilities and predisposing conditions that affect the likelihood that threat events of concern result in adverse impacts.

Task 2-4. **Determine Likelihood** – Determine the likelihood that threat events of concern result in adverse impacts, considering: 1) the characteristics of the threat sources that could initiate the events; 2) the vulnerabilities/predisposing conditions identified; and 3) the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

Task 2-5. **Determine Impact** – Determine the adverse impacts from threat events of concern, considering: 1) the characteristics of the threat sources that could initiate the events; 2) the vulnerabilities/predisposing conditions identified; and 3) the organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events.

Task 2-6. **Determine Risk** – Determine the risk to the organization from threat events of concern considering: 1) the impact that would result from the events; and 2) the likelihood of the events occurring.

*STEP 3: COMMUNICATE AND SHARE RISK ASSESSMENT RESULTS*

Task 3-1. **Communicate Risk Assessment Results** – Communicate risk assessment results to organizational decision makers to support risk responses.

Task 3-2. **Share Risk-Related Information** – Share risk-related information produced during the risk assessment with appropriate organizational personnel.

*STEP 4: MAINTAIN RISK ASSESSMENT*

Task 4-1. **Monitor Risk Factors** – Conduct ongoing monitoring of the risk factors that contribute to changes in risk to organizational operations and assets, individuals, other organizations, or the Nation.

Task 4-2. **Update Risk Assessment** – Update existing risk assessment using the results from ongoing monitoring of risk factors.

*APTA Recommended Practice Securing Control and Communications Systems in Transit Environments, Part 1* lists the “Stages of the Risk-Assessment Process” describing the major steps in organizing for and conducting a risk assessment for a transit agency:

1. **Generate Management Support and Empowerment for the Risk-Assessment Process** – Management support is necessary for the risk-assessment process. The process takes time and commitment, and empowerment and resources for the team are necessary.
2. **Form the Risk-Assessment Team from Technical Experts and Stakeholders** – The team that is formed should be of a combination of the organizational “owners” of these

areas, technical experts from these areas, and auxiliary groups. For instance a team might include Engineering, Operations, Maintenance, HR, Safety, IT, Security

3. **Identify Assets and Loss Impacts** – Determine the critical assets that require protection. This may include list of control and computing equipment, physical and network layouts, etc., and may include hard copy drawings, electronic network drawings, database printouts, etc. Keep this information in a secure central location for the team. Identify possible undesirable events and their impacts. Prioritize the assets based on consequence of loss.
4. **Identify Threats to Assets** – Identify source of potential threats to critical assets. Common threat sources include: Natural Threats—floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events. Human Threats—events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information). Environmental Threats—long-term power failure, pollution, chemicals, liquid leakage.
5. **Identify and Analyze Vulnerabilities** – Identify potential vulnerabilities related to specific assets or undesirable events. Identify existing countermeasures and their level of effectiveness in reducing vulnerabilities. Estimate the degree of vulnerability relative to each asset.
6. **Assess Risk and Determine Priorities for the Protection of Critical Assets** – Estimate the degree of impact relative to each critical asset. Estimate the likelihood of an attack by a potential threat. Likelihood is the probability that a particular vulnerability may be exploited by a potential threat (derived from NIST Risk Management Guide 800-53). Estimate the likelihood that a specific vulnerability will be exploited. This can be based on factors such as prior history or attacks on similar assets, intelligence, and warning from law enforcement agencies, consultant advice, the company’s own judgment, and additional factors. Prioritize risks based on an integrated assessment.
7. **Identify Countermeasures, Their Costs and Trade-Offs** – Identify potential countermeasures to reduce the vulnerabilities. Estimate the cost of the countermeasures. Conduct a cost-benefit and trade-off analysis. Prioritize options and recommendations for senior management.

Although there are currently very few cybersecurity risk assessment models specifically tailored to surface transportation assets or organizations, there are workable models and methodologies available for use in establishing the parameters by which cybersecurity risk will be evaluated. For example, the DHS ICS CERT Cybersecurity Evaluation Tool (CSET®) has been utilized by a number of transportation organizations to conduct assessments. Information about ICS-CERT is readily available at <https://ics-cert.us-cert.gov/Assessments>

The ICS CERT Assessment Program Overview as stated on the website reads:

*A core component of ICS-CERT's risk management mission is conducting security assessments in partnership with ICS stakeholders, including critical infrastructure owners and operators, ICS vendors, integrators, Sector-Specific Agencies, other Federal departments and agencies, SLTT governments, and international partners.*

*ICS-CERT works with these and other partners to assess various aspects of critical infrastructure (cybersecurity controls, control system architectures, and adherence to best practices supporting the resiliency, availability, and integrity of critical systems), and provides options for consideration to mitigate and manage risk.*

*ICS-CERT's assessment products improve situational awareness and provide insight, data, and identification of control systems threats and vulnerabilities. ICS-CERT's core assessment products and services include self-assessments using ICS-CERT's Cybersecurity Evaluation Tool (CSET®), onsite field assessments, network design architecture reviews, and network traffic analysis and verification. The information gained from assessments also provides stakeholders with the understanding and context necessary to build effective defense-in-depth processes for enhancing cybersecurity.*

Of course the underlying objective of the risk assessment is ensuring that the organization understands the cybersecurity risk to operations (including mission, functions, image, or reputation), organizational assets, and individuals.

A more detailed discussion of the three main areas of cybersecurity TVC analysis follows.

## Threat Assessment

In the cyber world *threats* are continually manifested, voluminous and subject to variation. Although there are identified primary types of threats such as “Stuxnet” a worm that attacks critical infrastructure, there are also characterizations of threat types including malware, short for malicious software, defined as any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems.

The National Institute of Standards and Technology's *Guide for Conducting Risk Assessments (NIST Special Publication 800-30 Revision 1, September 2012)* identifies threat event types under the category of adversarial/intentional acts as follows:

### 1. Perform reconnaissance and gather information

- a. Perform perimeter network reconnaissance/scanning. Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
- b. Perform network sniffing of exposed networks. Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing

to identify components, resources, and protections. Gather information using open source discovery of organizational information. Adversary mines publically accessible information to gather information about organizational information systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.

- c. Perform reconnaissance and surveillance of targeted organizations. Adversary uses various means (e.g., scanning, physical observation) over time to examine and assess organizations and ascertain points of vulnerability.
- d. Perform malware-directed internal reconnaissance. Adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.

## **2. Craft or create attack tools**

- a. Craft phishing attacks. Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.
- b. Craft spear phishing attacks. Adversary employs phishing attacks targeted at high value targets (e.g., senior leaders/executives).
- c. Craft attacks specifically based on deployed information technology environment. Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment.
- d. Create counterfeit/spoof website. Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.
- e. Craft counterfeit certificates. Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.
- f. Create and operate false front organizations to inject malicious components into the supply chain. Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life-cycle path that then inject corrupted/malicious information system components into the organizational supply chain

## **3. Deliver/insert/install malicious capabilities**

- a. Deliver known malware to internal organizational information systems (e.g., virus via email). Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e. g., malware whose existence is known) into organizational information systems.
- b. Deliver modified malware to internal organizational information systems. Adversary uses more sophisticated delivery mechanisms than email (e.g., web traffic, instant messaging, FTP) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.
- c. Deliver targeted malware for control of internal systems and exfiltration of data. Adversary installs malware that is specifically designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.

- d. Deliver malware by providing removable media. Adversary places removable media (e.g., flash drives) containing malware in locations external to organizational physical perimeters but where employees are likely to find the media (e.g., facilities parking lots, exhibits at conferences attended by employees) and use it on organizational information systems.
- e. Insert untargeted malware into downloadable software and/or into commercial information technology products. Adversary corrupts or inserts malware into common freeware, shareware or commercial information technology products. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.
- f. Insert targeted malware into organizational information systems and information system components. Adversary inserts malware into organizational information systems and information system components (e.g., commercial information technology products), specifically targeted to the hardware, software, and firmware used by organizations (based on knowledge gained via reconnaissance).
- g. Insert specialized malware into organizational information systems based on system configurations. Adversary inserts specialized, non-detectable, malware into organizational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organizational information systems.
- h. Insert counterfeit or tampered hardware into the supply chain. Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
- i. Insert tampered critical components into organizational systems. Adversary replaces, through supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
- j. Install general-purpose sniffers on organization controlled information systems or networks. Adversary installs sniffing software onto internal organizational information systems or networks.
- k. Install persistent and targeted sniffers on organizational information systems and networks. Adversary places within internal organizational information systems or networks software designed to (over a continuous period of time) collect (sniff) network traffic.
- l. Insert malicious scanning devices (e.g., wireless sniffers) inside facilities. Adversary uses postal service or other commercial delivery services to deliver to organizational mailrooms a device that is able to scan wireless communications accessible from within the mailrooms and then wirelessly transmit information back to adversary.
- m. Insert subverted individuals into organizations. Adversary places individuals within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions.
- n. Insert subverted individuals into privileged positions in organizations. Adversary places individuals in privileged positions within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files, etc.) and may leverage access to one

privileged capability to get to another capability.

#### 4. Exploit and compromise

- a. Exploit physical access of authorized staff to gain access to organizational facilities. Adversary follows (“tailgates”) authorized individuals into secure/controlled locations with the goal of gaining access to facilities, circumventing physical security checks.
- b. Exploit poorly configured or unauthorized information systems exposed to the Internet. Adversary gains access through the Internet to information systems that are not authorized for Internet connectivity or that do not meet organizational configuration requirements.
- c. Exploit split tunneling. Adversary takes advantage of external organizational or personal information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organizational information systems or networks and to non-secure remote connections.
- d. Exploit multi-tenancy in a cloud environment. Adversary, with processes running in an organizationally-used cloud environment, takes advantage of multi-tenancy to observe behavior of organizational processes, acquire organizational information, or interfere with the timely or correct functioning of organizational processes.
- e. Exploit known vulnerabilities in mobile systems (e.g., laptops, PDA’s, smart phones). Adversary takes advantage of fact that transportable information systems are outside physical protection of organizations and logical protection of corporate firewalls, and compromises the systems based on known vulnerabilities to gather information from those systems.
- f. Exploit recently discovered vulnerabilities. Adversary exploits recently discovered vulnerabilities in organizational information systems in an attempt to compromise the systems before mitigation measures are available or in place.
- g. Exploit vulnerabilities on internal organizational information systems. Adversary searches for known vulnerabilities in organizational internal information systems and exploits those vulnerabilities.
- h. Exploit vulnerabilities using zero-day attacks. Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and applications used by organizations as well as adversary reconnaissance of organizations.
- i. Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo. Adversary launches attacks on organizations in a time and manner consistent with organizational needs to conduct mission/business operations.
- j. Exploit insecure or incomplete data deletion in multitenant environment. Adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment (e.g., in a cloud computing environment).
- k. Violate isolation in multi-tenant environment. Adversary circumvents or defeats isolation mechanisms in a multi-tenant environment (e.g., in a cloud computing environment) to observe, corrupt, or deny service to hosted services and information/data.
- l. Compromise critical information systems via physical access. Adversary obtains physical access to organizational information systems and makes modifications.

- m. Compromise information systems or devices used externally and reintroduced into the enterprise. Adversary installs malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected.
- n. Compromise software of organizational critical information systems. Adversary inserts malware or otherwise corrupts critical internal organizational information systems.
- o. Compromise organizational information systems to facilitate exfiltration of data/information. Adversary implants malware into internal organizational information systems, where the malware over time can identify and then exfiltrate valuable information.
- p. Compromise mission-critical information. Adversary compromises the integrity of mission-critical information, thus preventing or impeding ability of organizations to which information is supplied, from carrying out operations.
- q. Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware). Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.

**5. Conduct an attack (i.e., direct/coordinate attack tools or activities)**

- a. Conduct communications interception attacks. Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publically known flaws), targets those communications, and gains access to transmitted information and channels.
- b. Conduct wireless jamming attacks. Adversary takes measures to interfere with wireless communications so as to impede or prevent communications from reaching intended recipients.
- c. Conduct attacks using unauthorized ports, protocols and services. Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorized for use by organizations.
- d. Conduct attacks leveraging traffic/data movement allowed across perimeter. Adversary makes use of permitted information flows (e.g., email communication, removable storage) to compromise internal information systems, which allows adversary to obtain and exfiltrate sensitive information through perimeters.
- e. Conduct simple Denial of Service (DoS) attack. Adversary attempts to make an Internet-accessible resource unavailable to intended users, or prevent the resource from functioning efficiently or at all, temporarily or indefinitely.
- f. Conduct Distributed Denial of Service (DDoS) attacks. Adversary uses multiple compromised information systems to attack a single target, thereby causing denial of service for users of the targeted information systems. Conduct targeted Denial of Service (DoS) attacks. Adversary targets DoS attacks to critical information systems, components, or supporting infrastructures, based on adversary knowledge of dependencies.
- g. Conduct physical attacks on organizational facilities. Adversary conducts a physical attack on organizational facilities (e.g., sets a fire).
- h. Conduct physical attacks on infrastructures supporting organizational facilities. Adversary conducts a physical attack on one or more infrastructures supporting

- organizational facilities (e.g., breaks a water main, cuts a power line).
- i. Conduct cyber-physical attacks on organizational facilities. Adversary conducts a cyber-physical attack on organizational facilities (e.g., remotely changes HVAC settings).
  - j. Conduct data scavenging attacks in a cloud environment. Adversary obtains data used and then deleted by organizational processes running in a cloud environment.
  - k. Conduct brute force login attempts/password guessing attacks. Adversary attempts to gain access to organizational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities. Conduct non-targeted zero-day attacks. Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Attacks are not based on any adversary insights into specific vulnerabilities of organizations.
  - l. Conduct externally-based session hijacking. Adversary takes control of (hijacks) already established, legitimate information system sessions between organizations and external entities (e.g., users connecting from off-site locations).
  - m. Conduct internally-based session hijacking. Adversary places an entity within organizations in order to gain access to organizational information systems or networks for the express purpose of taking control (hijacking) an already established, legitimate session either between organizations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.
  - n. Conduct externally-based network traffic modification (man in the middle) attacks. Adversary, operating outside organizational systems, intercepts/eavesdrops on sessions between organizational and external systems. Adversary then relays messages between organizational and external systems, making them believe that they are talking directly to each other over a private connection, when in fact the entire communication is controlled by the adversary. Such attacks are of particular concern for organizational use of community, hybrid, and public clouds.
  - o. Conduct internally-based network traffic modification (man in the middle) attacks. Adversary operating within the organizational infrastructure intercepts and corrupts data sessions.
  - p. Conduct outsider-based social engineering to obtain information. Externally placed adversary takes actions (e.g., using email, phone) with the intent of persuading or otherwise tricking individuals within organizations into revealing critical/sensitive information (e.g., personally identifiable information).
  - q. Conduct insider-based social engineering to obtain information. Internally placed adversary takes actions (e.g., using email, phone) so that individuals within organizations reveal critical/sensitive information (e.g., mission information).
  - r. Conduct attacks targeting and compromising personal devices of critical employees. Adversary targets key organizational employees by placing malware on their personally owned information systems and devices (e.g., laptop/notebook computers, personal digital assistants, smart phones). The intent is to take advantage of any instances where employees use personal information systems or devices to handle critical/sensitive information.
  - s. Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware. Adversary targets and compromises the operation of software (e.g.,



through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components.

**6. Achieve results (i.e., cause adverse impacts, obtain information)**

- a. Obtain sensitive information through network sniffing of external networks. Adversary with access to exposed wired or wireless data channels that organizations (or organizational personnel) use to transmit information (e.g., kiosks, public wireless networks) intercepts communications.
- b. Obtain sensitive information via exfiltration. Adversary directs malware on organizational systems to locate and surreptitiously transmit sensitive information.
- c. Cause degradation or denial of attacker-selected services or capabilities. Adversary directs malware on organizational systems to impair the correct and timely support of organizational mission/business functions.
- d. Cause deterioration/destruction of critical information system components and functions. Adversary destroys or causes deterioration of critical information system components to impede or eliminate organizational ability to carry out missions or business functions. Detection of this action is not a concern.
- e. Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement). Adversary vandalizes, or otherwise makes unauthorized changes to, organizational websites or data on websites.
- f. Cause integrity loss by polluting or corrupting critical data. Adversary implants corrupted and incorrect data in critical data, resulting in suboptimal actions or loss of confidence in organizational data/services.
- g. Cause integrity loss by injecting false but believable data into organizational information systems. Adversary injects false but believable data into organizational information systems, resulting in suboptimal actions or loss of confidence in organizational data/services.
- h. Cause disclosure of critical and/or sensitive information by authorized users. Adversary induces (e.g., via social engineering) authorized users to inadvertently expose, disclose, or mishandle critical/sensitive information.
- i. Cause unauthorized disclosure and/or unavailability by spilling sensitive information. Adversary contaminates organizational information systems (including devices and networks) by causing them to handle information of a classification/sensitivity for which they have not been authorized. The information is exposed to individuals who are not authorized access to such information, and the information system, device, or network is unavailable while the spill is investigated and mitigated.
- j. Obtain information by externally located interception of wireless network traffic. Adversary intercepts organizational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organizational wireless routers.
- k. Obtain unauthorized access. Adversary with authorized access to organizational information systems, gains access to resources that exceeds authorization.
- l. Obtain sensitive data/information from publicly accessible information systems. Adversary scans or mines information on publically accessible servers and web

pages of organizations with the intent of finding sensitive information.

- m. Obtain information by opportunistically stealing or scavenging information systems/components. Adversary steals information systems or components (e. g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organizations, or scavenges discarded components.

#### **7. Maintain a presence or set of capabilities**

- a. Obfuscate adversary actions. Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations.
- b. Adapt cyber attacks based on detailed surveillance. Adversary adapts behavior in response to surveillance and organizational security measures.

#### **8. Coordinate a campaign**

- a. Coordinate a campaign of multi-staged attacks (e.g., hopping). Adversary moves the source of malicious commands or actions from one compromised information system to another, making analysis difficult.
- b. Coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies. Adversary combines attacks that require both physical presence within organizational facilities and cyber methods to achieve success. Physical attack steps may be as simple as convincing maintenance personnel to leave doors or cabinets open.
- c. Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome. Adversary does not limit planning to the targeting of one organization. Adversary observes multiple organizations to acquire necessary information on targets of interest.
- d. Coordinate a campaign that spreads attacks across organizational systems from existing presence. Adversary uses existing presence within organizational systems to extend the adversary's span of control to other organizational systems including organizational infrastructure. Adversary thus is in position to further undermine organizational ability to carry out missions/business functions.
- e. Coordinate a campaign of continuous, adaptive, and changing cyber attacks based on detailed surveillance. Adversary attacks continually change in response to surveillance and organizational security measures.
- f. Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors. Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organizational operations.

***NIST Special Publication 800-30*** lists non-adversarial threat events as:

1. Spill sensitive information. Authorized user erroneously contaminates a device, information system, or network by placing on it or sending to it information of a classification/sensitivity which it has not been authorized to handle. The information is exposed to access by unauthorized individuals, and as a result, the device, system, or network is unavailable while the spill is investigated and mitigated.
2. Mishandling of critical and/or sensitive information by authorized users. Authorized privileged user inadvertently exposes critical/sensitive information.
3. Incorrect privilege settings. Authorized privileged user or administrator erroneously assigns a user exceptional privileges or sets privilege requirements on a resource too

- low.
4. Communications contention. Degraded communications performance due to contention.
  5. Unreadable display. Display unreadable due to aging equipment.
  6. Earthquake at primary facility. Earthquake of organization-defined magnitude at primary facility makes facility inoperable.
  7. Fire at primary facility. Fire (not due to adversarial activity) at primary facility makes facility inoperable.
  8. Fire at backup facility. Fire (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
  9. Flood at primary facility. Flood (not due to adversarial activity) at primary facility makes facility inoperable.
  10. Flood at backup facility. Flood (not due to adversarial activity) at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
  11. Hurricane at primary facility. Hurricane of organization-defined strength at primary facility makes facility inoperable.
  12. Hurricane at backup facility. Hurricane of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.
  13. Resource depletion. Degraded processing performance due to resource depletion.
  14. Introduction of vulnerabilities into software products. Due to inherent weaknesses in programming languages and software development environments, errors and vulnerabilities are introduced into commonly used software products.
  15. Disk error. Corrupted storage due to a disk error.
  16. Pervasive disk error. Multiple disk errors due to aging of a set of devices all acquired at the same time, from the same supplier.
  17. Windstorm/tornado at primary facility. Windstorm/tornado of organization-defined strength at primary facility makes facility inoperable.
  18. Windstorm/tornado at backup facility. Windstorm/tornado of organization-defined strength at backup facility makes facility inoperable or destroys backups of software, configurations, data, and/or logs.

## Vulnerability Assessment

In the strictest sense, a vulnerability is basically a weakness in an information system or the procedures, controls or implementation processes surrounding the system that can be exploited by an intentional actor or compromised by non-adversarial error, natural events or accident. Generally, information system vulnerabilities result from lapses in security controls. However, the exploitation of vulnerabilities has been increasingly enabled by rapidly emerging changes in technology or changes in organizational operations or mission. Successful exploitation of a vulnerability is a function of three inter-related elements: a susceptibility of the information system itself to attack; an available means to access the system's specific security control lapse or vulnerability; and the capability of an adversary to carry out the actions necessary to exploit the information system.

However as *NIST Special Publication 800-30* points out, “vulnerabilities are not identified only within information systems...vulnerabilities can be found in organizational governance structures (e.g., the lack of effective risk management strategies and adequate risk framing, poor intra- agency communications, inconsistent decisions about relative priorities of missions/business functions, or misalignment of enterprise architecture to support mission/business activities)... or in external relationships (e.g., dependencies on particular energy sources, supply chains, information technologies, and telecommunications providers), mission/business processes (e.g., poorly defined processes or processes that are not risk-aware), and enterprise/information security architectures (e.g., poor architectural decisions resulting in lack of diversity or resiliency in organizational information systems).”

Whether caused by internal flaws to information systems or more broadly by inadequate business practices or supply chain weaknesses, it is essential that transportation organizations understand the extent of their current and future reliance on information systems, the vulnerabilities of these systems, and how to mitigate the vulnerabilities associated with their utilization.

#### *Common Vulnerabilities of Information Systems*

The list of vulnerabilities for IT systems is far too voluminous and fluid to be included in the research. However, the information is readily available. The *National Vulnerability Database* (<https://nvd.nist.gov>) currently contains a listing of more than 71, 429 CVE's (Common Vulnerabilities and Exposures). The NVD is the U.S. government repository of standards based vulnerability management data. The CVE is a list or dictionary of standardized identifiers for common computer vulnerabilities or exposures. CVE is complimentary and publicly available. Information in the CVE is organized by year, beginning with 1999. It is available for download in numerous formats CVRF, HTML, XML, and Text.

#### *Common Vulnerabilities of Industrial Control Systems*

In 2001 the U.S. Department of Homeland Security published the document, *Common Cybersecurity Vulnerabilities in Industrial Control Systems*. The report provides a useful summary of information system vulnerabilities. The information is sub-divided into three categories: 1) vulnerabilities inherent in the ICS product; 2) vulnerabilities caused during the installation, configuration, and maintenance of the ICS; and 3) the lack of adequate protection because of poor network design or configuration.

##### 1. Vulnerabilities Inherent in the ICS Product

- a. **Improper Input Validation.** Input validation is used to ensure that the content provided to an application does not grant an attacker access to unintended functionality or privilege escalation.
  - i. Buffer overflows. Buffer overflows result when a program tries to write more data into a buffer than the space allocated in memory. The “extra” data then overwrite adjacent memory and ultimately result in abnormal

operation of the program. A careful and successful memory overwrite can cause the program to begin execution of actual code submitted by the attacker. Most exploit code allows the attacker to create an interactive session and send commands with the privileges of the program with the buffer overflow. When network protocols have been implemented without validating the input values, these protocols can be vulnerable to buffer overflow attacks. Buffer overflows are the most common type of vulnerability identified in ICS products.

- ii. **Lack of Bounds Checking.** The lack of input validation for values that are expected to be in a certain range, such as array index values, can cause unexpected behavior. For instance, invalidated input, negative, or too large numbers can be input for array access and cause essential services to crash. ICS applications frequently suffer from coding practices that allow attackers to supply unexpected data and thus modify program execution. Even though ICS applications pass valid data values during normal operation, a common vulnerability discovery approach is to alter or input unexpected values. Types of exploitation can include DoS caused by out-of-range index values, crashed ICS communications service by altering the input value to negative number and crashed proprietary fault tolerant network equipment protocol.
- iii. **Command Injection.** Command injection allows for the execution of arbitrary commands and code by the attacker. If a malicious user injects a character (such as a semi-colon) that delimits the end of one command and the beginning of another, it may be possible to then insert an entirely new and unrelated command that was not intended to be executed.
- iv. **SQL Injection.** SQL command injection has become a common issue with database-driven websites. The flaw is easily detected and easily exploited, and as such, any site or software package with even a minimal user base is likely to be subject to an attempted attack of this kind. This flaw depends on the fact that SQL makes no real distinction between the control and data planes.
- v. **Cross-Site Scripting.** Cross-site scripting vulnerabilities allow attackers to inject code into the web pages generated by the vulnerable web application. Attack code is executed on the client with the privileges of the web server. The root cause of a cross-site scripting (XSS) vulnerability is the same as that of an SQL injection, poorly sanitized data. However, a XSS attack is unique in the sense that the web application itself unwittingly sends the malicious code to the user. The most common attack performed with cross-site scripting involves the disclosure of information stored in user cookies. Because the site requesting to run the script has access to the cookies in question, the malicious script does also. Some cross-site scripting vulnerabilities can be exploited to manipulate or steal cookies, create requests that can be mistaken for those of a valid user, compromise confidential information, or execute malicious code on the end user systems.
- vi. **Improper Limitation of a Pathname to a Restricted Directory (Path**

Traversal). Directory traversal vulnerabilities occur when file paths are not validated. Directory traversals occur when the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory. However, the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. The attacker may be able to read, overwrite, or create critical files such as programs, libraries, or important data. This may allow an attacker to execute unauthorized code or commands, read or modify files or directories, crash, exit, or restart critical files or programs, potentially causing a DoS.

- b. **Poor Code Quality.** Poor code quality refers to code issues that are not necessarily vulnerabilities, but indicate that it was not carefully developed or maintained. These products are more likely to contain vulnerabilities than those that were developed using secure development concepts and other good programming practices.
  - i. Use of Potentially Dangerous Functions. Otherwise known as unsafe function calls, the application calls a potentially dangerous function that could introduce vulnerability if used incorrectly.
  - ii. NULL Pointer Dereference. A NULL pointer dereference occurs when the application dereferences a pointer that it expects to be valid, but is NULL, typically causing a crash or exit. NULL pointer dereference issues can occur through a number of flaws, including race conditions, and simple programming omissions.
- c. **Permissions, Privileges, and Access Controls.** Permissions, privileges, and other security features are used to perform access controls on computer systems. Missing or weak access controls can be exploited by attackers to gain unauthorized access to ICS functions.
  - i. Improper Access Control (Authorization). If ICS software does not perform or incorrectly performs access control checks across all potential execution paths, users are able to access data or perform actions that they should not be allowed to perform. Specific security control lapses: 1) access is not restricted to the objects that require it; 2) ICS protocol allowed ICS system hosts to read or overwrite files on other hosts, without any logging; 3) documentation and configuration information is shared freely (read only); 4) common shares are available on multiple systems; 5) lack of role-based authentication for ICS component communication; 6) a remote user can upload a file to any location on the targeted computer; 7) arbitrary file download is allowed on ICS hosts; 8) arbitrary file upload is allowed on ICS hosts; 9) remote client is allowed to launch any process; 10) ICS service allows anonymous access; 11) undisclosed “back door” administrative accounts.
  - ii. Execution with Unnecessary Privileges. Services are restricted to the user rights granted through the user account associated with them. Exploitation of any service could allow an attacker a foothold on the ICS network with the exploited service’s permissions. Privilege escalation can be accomplished by

exploiting a vulnerable service running with more privileges than the attacker has currently obtained.

- d. **Improper Authentication.** Many vulnerabilities identified in ICS products are due to the ICS software failing to sufficiently verify a claim to have a given identity.
- i. **Authentication Bypass Issues.** The software does not properly perform authentication, allowing it to be bypassed through various methods. Web services developed for the ICS tend to be vulnerable to attacks that can exploit the ICS Web server to gain unauthorized access. System architectures often use network DMZ's to protect critical systems and to limit exposure of network components. Vulnerabilities in ICS DMZ Web servers may provide the first step in the attack path by allowing access within the ICS exterior boundary. Vulnerabilities in lower level component's web servers can provide more steps in the attack path.
  - ii. **Missing Authentication for Critical Function.** The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources. Many critical ICS functions do not require authentication. Exposing critical functionality essentially provides an attacker with the privilege level of that functionality. The consequences will depend on the associated functionality, but they can range from reading or modifying sensitive data, access to administrative or other privileged functionality, or execution of arbitrary code.
  - iii. **Client-Side Enforcement of Server-Side Security.** Applications that authenticate users locally trust the client that is connecting to a server to perform the authentication. Because the information needed to authenticate is stored on the client side, a moderately skilled hacker may easily extract that information or modify the client to not require authentication. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.
  - iv. **Channel Accessible by Non-endpoint (Man-In-The-Middle).** Commands from the HMI cause actions in the ICS. Alarms are sent to the HMI that notify operators of triggered events. The integrity and timely delivery of alarms and commands are critical in an ICS. MitM is possible if the ICS does not adequately verify the identity of actors at both ends of a communication channel, or does not adequately ensure the integrity of the channel, in a way that allows the channel to be accessed or influenced by an actor that is not an endpoint. Inadequate or inconsistent verification may result in insufficient or incorrect identification of either communicating entity. This can have negative consequences such as misplaced trust in the entity at the other end of the channel. An attacker can leverage this by interposing between the communicating entities and masquerading as the original entity. In the absence of sufficient verification of identity, such an attacker can eavesdrop and potentially modify the communication between the original entities. Weak authentication in ICS protocols allows replay or spoof attacks to send unauthorized messages and a possibility of sending messages that update the HMI or remote terminal unit must be

considered. The attacker may be able to cause invalid data to be displayed on a console or create invalid commands or alarm messages. Clear-text authentication credentials can be sniffed and used by an attacker to authenticate to the system.

- e. **Insufficient Verification of Data Authenticity.** If ICS protocols and software do not sufficiently verify the origin or authenticity of data, it may accept invalid data. This is a serious risk for systems that rely on data integrity.
  - i. **Cross-Site Request Forgery.** When a web server is designed to receive a request from a client without any mechanism for verifying that it was intentionally sent, then it might be possible for an attacker to trick a client into making an unintentional request to the web server that will be treated as an authentic request. If the web interface offers a way to change ICS settings, hijacking credentials using cross-site request forgery (CSRF) could give an attacker the ability to perform any task that a legitimate user would be able to do through the web interface.
  - ii. **Missing Support for Integrity Check.** Many ICS transmission protocols do not include a mechanism for verifying the integrity of the data during transmission. If integrity check values or “checksums” are omitted from a protocol, there is no way of determining if data have been corrupted in transmission. The lack of checksum functionality in a protocol removes the first application-level check of data that can be used. The end-to-end philosophy of checks states that integrity checks should be performed at the lowest level that they can be completely implemented. Excluding further sanity checks and input validation performed by applications, the protocol's checksum is the most important level of checksum, because it can be performed more completely than at any previous level and takes into account entire messages, as opposed to single packets.
  - iii. **Download of Code without Integrity Check.** If an ICS component downloads source code or an executable from the network and executes the code without sufficiently verifying the origin and integrity of the code, an attacker may be able to execute malicious code by compromising the host server, spoofing an authorized server, or modifying the code in transit.

**f. Cryptographic Issues**

- i. **Missing Encryption of Sensitive Data.** Credentials sent across the network in clear text leave the system at risk to the unauthorized use of a legitimate user's credentials. If attackers are able to capture usernames and passwords, they will be able to log onto the system with that user's privileges. Any unencrypted information concerning the ICS source code, topology, or devices is a potential benefit for an attacker and should be limited. One of the greatest security issues identified in conjunction with ICS systems is the widespread use of unencrypted plain-text network communications protocols. Many applications and services use protocols that include human-readable characters and strings. Network sniffing tools, many of



which are freely downloadable, can be used to view this type of network traffic. As a result, the content of the ICS communication packets can be intercepted, read, and manipulated. Vulnerable data in this scenario include usernames, passwords, and ICS commands.

**g. Credentials Management**

- i. **Insufficiently Protected Credentials.** Credentials sent across the network in clear text leave the system at risk to the unauthorized use of a legitimate user's credentials. Network sniffing tools, many of which are freely downloadable, can be used to view this type of network traffic. If attackers are able to capture usernames and passwords, they will be able to log onto the system with that user's privileges. Unsecure services developed for IT systems have been adopted for use in ICS for common IT functionality. Although more secure alternatives exist for most of these services, some ICS's have these services integrated into their applications.
- ii. **Use of Hard-Coded Credentials.** Hard-coded credentials have been found in ICS code and configuration scripts for authentication between ICS components. In such cases authentication may not be required to read system configuration file, which contains user accounts details, including passwords.

**h. ICS Software Security Configuration and Maintenance (Development)**

- i. **Poor Patch Management.** During ICS Software Development Vulnerabilities in ICS can occur because of flaws, misconfigurations, or poor maintenance of their platforms, including hardware, operating systems, and ICS applications. These vulnerabilities can be mitigated through various security controls, such as operating system and application patching, physical access control, and security software (e.g., antivirus software). A computer system is vulnerable to attack from the time a vulnerability is discovered and publicly disclosed, to when a patch is generated, disseminated, and finally applied. The number of publicly announced vulnerabilities has been steadily increasing over the past decade to the point where patch management is a necessary part of maintaining a computer system. Although patching may be difficult in high-availability environments, unpatched systems are often trivial to exploit due to the ease of recognizing product version and the readiness of exploit code.
- ii. **Unpatched or Old Versions of Third-party Applications Incorporated into ICS Software.** These applications possess vulnerabilities that may provide an attack path into the system. The software is well known, and available exploit code makes them an easy target.
- iii. **Improper Security Configuration.** Many weaknesses identified in ICS software are because of available security options not being used or enabled.

**2. Vulnerabilities Caused During Installation/Configuration/Maintenance of ICS.**

**a. Permissions, Privileges, and Access Controls**

- i. **Poor System Access Controls.** Within access controls, the following common vulnerabilities have been identified: 1) lack of separation of duties

through assigned access authorization, 2) lack of lockout system enforcement for failed login attempts, and 3) terminated remote access sessions after a defined time period.

- ii. Open Network Shares on ICS Hosts. The storage of ICS artifacts, such as source code and system configuration on a shared file system, provides significant potential for information mining by an attacker. The design of many ICS requires open network shares on ICS hosts.

**b. Improper Authentication**

- i. Poor System Identification/Authentication Controls. Lack of developed policies or procedures to facilitate the implementation of identification and authentication controls. Absence of unique identification and authentication for users and specific devices before establishing connections.

**c. Credentials Management**

- i. Insufficiently Protected Credentials User. Credentials should be vigorously protected and made inaccessible to an attacker. Whenever credentials are passed in clear text, they are susceptible to being captured and then cracked if necessary by the attacker. If stored password hashes are not properly protected, they may be accessed by an attacker and cracked. In every case, the lack of protection of user credentials may lead to the attacker gaining increased privileges on the ICS and thus being able to more effectively advance the attack.
- ii. Weak Passwords. ICS systems have been configured without passwords, which means that anyone able to access these applications are guaranteed to be able to authenticate and interact with them.

**d. ICS Security Configuration and Maintenance**

- i. Weak Testing Environments. Patch management is paramount to maintaining the integrity of both IT and ICS. Unpatched software represents one of the greatest vulnerabilities to a system. Software updates on IT systems, including security patches, are typically applied in a timely fashion based on appropriate security policy and procedures. In addition, these procedures are often automated using server-based tools. Software updates on ICS cannot always be implemented on a timely basis because these updates need to be thoroughly tested by the vendor of the industrial control application and the end user of the application before being implemented. ICS outages often must be planned and scheduled days/weeks in advance. The ICS may also require revalidation as part of the update process. Another issue is that many ICS use older versions of operating systems that are no longer supported by the vendor. Consequently, available patches may not be applicable. Change management is also applicable to hardware and firmware. The change management process, when applied to ICS, requires careful assessment by ICS experts (e.g., control engineers) working in conjunction with security and IT personnel. Vulnerabilities that have had patches available for a long time are still being seen on ICS. Unpatched operating systems open ICS to attack through known operating system service vulnerabilities.
- ii. Limited Patch Management Abilities. Many ICS facilities, especially

smaller facilities, have no test facilities, so security changes must be implemented using the live operational systems.

- iii. **Weak Backup and Restore Abilities.** Backups, restores, and testing environments have been identified as a common issue within the industry for continuity of operations in the event of an incident. Backups are usually made, but usually not stored offsite and rarely exercised and tested.

**e. Planning/Policy/Procedures**

- i. **Insufficient Security Documentation.** A common security gap is the failure of an organization to establish a formal business case for ICS security or to develop, implement, disseminate, and periodically review/update policy and procedures to facilitate implementation of security planning controls.

**f. Audit and Accountability**

- i. **Lack of Security Audits/Assessments.** Security audits should be regularly performed to determine the adequacy of security controls within their systems.
- ii. **Lack of Logging or Poor Logging Practices Event.** Logging (applications, events, login activities, security attributes, etc.) is not turned on or monitored for identification of security issues. Where logs and other security sensors are installed, they may not be monitored on a real-time basis, and therefore, security incidents may not be rapidly detected and countered.

**3. Vulnerabilities Caused by Lack of Adequate Protection Because of Poor Network Design or Configuration.**

**a. Common ICS Network Design Weaknesses.** The network infrastructure environment within the ICS has often been developed and modified based on business and operational requirements, with little consideration for the potential security impacts of the changes. Over time, security gaps may have been inadvertently introduced within particular portions of the infrastructure. Without remediation, these gaps may represent backdoors into the ICS.

- i. **No Security Perimeter Defined.** If the control network does not have a security perimeter clearly defined, then it is not possible to ensure that the necessary security controls are deployed and configured properly. This can lead to unauthorized access to systems and data as well as other problems.
- ii. **Lack of Network Segmentation.** Minimal or no security zones allow vulnerabilities and exploitations to gain immediate full control of the systems, which could cause high-level consequences.
- iii. **Lack of Functional DMZs.** The use of several DMZs provides the added capability to separate functionalities and access privileges and has proved to be very effective in protecting large architectures composed of networks with different operational mandates.
- iv. **Firewalls Nonexistent or Improperly Configured.** A lack of properly configured firewalls could permit unnecessary data to pass between networks such as control and corporate networks. This could cause several problems, including allowing attacks and malware to spread

between networks, making sensitive data susceptible to monitoring/eavesdropping on the other network, and providing individuals with unauthorized access to systems.

- v. **Firewall Bypassed.** Backdoor network access is not recommended and could cause direct access to ICS for attackers to exploit and take full control of the system. All connections to the ICS LAN should be routed through the firewall. No hardwired connections should be circumventing the firewall.
- vi. **Weak Firewall Rules.** Firewall rules are the implementation of the network design. Enforcement of network access permissions and allowed message types and content is executed by firewall rules. Firewall rules determine which network packets are allowed in and out of a network. Packets can be filtered based on IP address, port number, direction, and content. The protection provided by a firewall depends on the rules it is configured to use. Firewall and router filtering deficiencies allow access to ICS components through external and internal networks. The lack of incoming access restrictions creates access paths into critical networks. The lack of outgoing access restrictions allows access from internal components that may have been compromised. For an attacker to remotely control exploit code running on the user's computer, a return connection must be established from the victim network. If outbound filtering is implemented correctly, the attacker will not receive this return connection and cannot control the exploited machine. Firewall rules should restrict traffic flow as much as possible. Connections should normally not be initiated from less-trusted networks.
- vii. **Access to Specific Ports on Host Not Restricted to Required IP Addresses.** This common vulnerability involves firewall rules restricting access to specific ports, but not IP addresses. Network device access control lists should restrict access to the required IP addresses. Allowing access to unused IP addresses traceable to legacy configuration of the firewall illuminates an attack path by using this IP address in order to be allowed through the firewall.
- viii. **Firewall Rules Are Not Tailored to ICS Traffic.** ICS network administrators should restrict communications to only that necessary for system functionality. System traffic should be monitored, and rules should be developed that allow only necessary access. Any exceptions created in the firewall rule set should be as specific as possible, including host, protocol, and port information.

**b. ICS Network Component Configuration (Implementation) Vulnerabilities**

- i. **Network Devices Not Securely Configured.** Network device access control lists should restrict access to the required IP addresses. Network devices configured to allow remote management over clear-text authentication protocols can result in an attacker gaining control by changing the network device configurations.
- ii. **Port Security Not Implemented on Network Equipment.** Unauthorized

network access through physical access to network equipment includes the lack of physical access control to the equipment, including the lack of security configuration functions that limit functionality even if physical access is obtained. A malicious user who has physical access to an unsecured port on a network switch could plug into the network behind the firewall to defeat its incoming filtering protection.

**c. Audit and Accountability**

- i. Network Architecture Not Well Understood. The current network diagram does not match the current state of the ICS network.
- ii. Weak Enforcement of Remote Login Policies. Any connection into the ICS LAN is considered part of the perimeter. Often these perimeters are not well documented, and some connections are neglected.
- iii. Weak Control of Incoming and Outgoing Media. Media protections for ICS lack written and approved policies and procedures, lack control of incoming and outgoing media, and lack verification scans of all allowed media into the ICS environment.
- iv. Lack of or Poor Monitoring of IDS's. Intrusion detection deployments apply different rule-sets and signatures unique to each domain being monitored.

## Consequence or Impact Assessment

Consequence analysis is basically an assessment of the perceived impact of an adverse event or series of events on critical infrastructure or processes. In regards to information systems, the level of impact is attributable to the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. Unfortunately in the transportation environment involves a potential for loss of life or serious injury based on the adverse effects of compromised, agency controlled or operated SCADA or ICS systems. Indeed transportation system operators are faced with a “duty of care” for system users that extends beyond the typical cyber breach.

The APTA Leadership Class 2013 undertook a project to examine issues associated with cybersecurity in transit. In regards to impact the authors described the extent of the concerns as follows:

*Politically motivated attacks against a transit agency can generally be expected to have an impact anywhere along a spectrum of casualty, depending on the motivation for the attack, from minor disruption to complete destruction. The worst case scenario is, of course, a politically motivated attack intended to terrorize and that disables or destroys a transit agency's systems in such a way that there is loss of life and injury to employees, passengers and the general public. In a classic case of 'insult to injury', on top of the loss of human life that cannot be replaced and physical assets that must be rebuilt, the transit agency and its surrounding community are likely to suffer long-term psychological and economic damage as a direct result. Other*

*political cyber attacks may result in disruption of major systems without loss of life, but with consequent financial damage, or in disruption of minor systems that serve mainly to annoy or cause public relations damage. The political attacks against transportation systems described in this report resulted in defaced web sites, compromised user credentials and some disruption to operations. One attack, whose motivation is not known, did have the potential to result in loss of life and destruction of major infrastructure. Financially motivated attacks can result in a transit agency losing cash resources, but perhaps more likely, a particular kind of data is the asset sought by the criminal hacker - data that is marketable as an asset on the black market. This data, commonly referred to as personally identifiable information or PII, belongs to the transit agency's employees and customers not the transit agency itself. The damage resulting from this sort of breach can include liability for violation of federal and state confidentiality laws, civil suits for identity theft resulting from a failure to reasonably safeguard PII, and a loss of confidence in the transit agency on the part of its customers resulting in their refusal to utilize the very types of technologies that transit agencies increasingly depend upon for operational efficiencies, such as electronic ticketing, automatic renewal of passes and social media tools. Every transit executive should be aware whether his or her agency's assets can be destroyed or disabled if its IT systems are subject to a cyber-based terror attack and should be kept informed of the agency's planned response to any such attack. Additionally, a transit agency executive should know whether his or her agency obtains and keeps the type of data that criminals have stolen from other state and local government entities and how the agency ensures that such data is kept secure from a cyber breach.*

Traditional consequence analysis begins with the delineation of the full complement of organizational assets into those that are considered critical to business operations. In the case of information system critical infrastructure this has spawned the designation of "CIIP" (Critical Information Infrastructure Protection) as a subset of the more widely-known concept of Critical Infrastructure Protection (CIP) (Peter Burnett Meridian Coordinator, CiviPol Consultant Quarter House Ltd). Tongue-in-cheek irrespective of what it is called, critical asset identification is related to the protection of the energy, telecommunications, water supply, transport, finance, health and other infrastructures that allow a society to function.

*"These critical infrastructures need to be protected against accidental and deliberate events that would stop them operating correctly and would severely impact the economic and social well-being." (Burnett)*

Unfortunately at present there is no fully developed listing of foundational cyber critical assets for surface transportation organizations. Volpe in collaboration with DHS is currently working on such a designation, however the effort remains a work in process. **APTA**

*Cybersecurity Considerations for Public Transit* does provide a very useful grouping of critical assets in transit into three main categories. The transit IT “ecosystem” and definitions for each of the categories follows:



Figure 4: Transportation Information Ecosystem. From APTA Cybersecurity Considerations for Public Transit

**Operational systems:** These systems integrate supervisory control and data acquisition (SCADA), original equipment manufacturer (OEM) and other critical component technologies responsible for the control, movement and monitoring of transportation equipment and services (i.e., train, track and signal control). Often such systems are interrelated into multimodal systems such as buses, ferries and metro modes.

**Enterprise information systems.** This describes the transit agency’s information system, which consist of integrated layers of the operating system, applications system and business system. Holistically, enterprise information systems encompass the entire range of internal and external information exchange and management.

**Subscribed systems:** These consist of “managed” systems outside the transportation agency. Such systems may include Internet service providers (ISPs), hosted networks, the agency website, data storage, cloud services, etc.

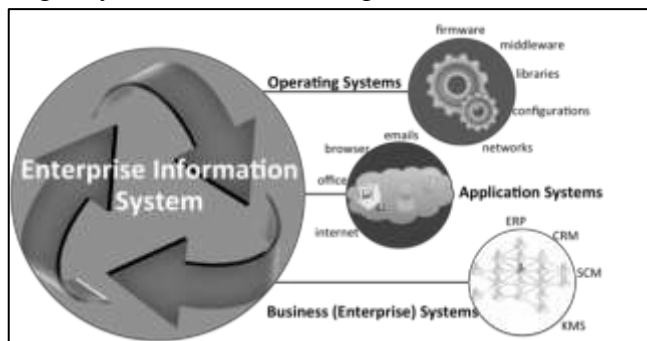


Figure 5: Transportation Enterprise Information Systems. From APTA Cybersecurity Considerations for Public Transit

Examples include control systems that support operational systems, SCADA, traction power control, emergency ventilation control, alarms and indications, fire/intrusion detection systems, train control/signaling, fare collection, automatic vehicle location (AVL), physical security feeds (CCTV, access control), public information systems, public address systems, and radio/wireless/related communication. Networks for traffic

management, yard management, crew management, vehicle management, vehicle maintenance, positive train control, traffic control, and remote railway switch control, main line work orders, wayside maintenance, on-track maintenance, intermodal operations, threat management and passenger services. And business management systems that support administrative processes including transaction processing systems, management information systems, decision support, executive support, financial pay systems, HR, training, and knowledge management.

*NIST Special Publication 800-30* guidelines recommend identifying information system critical assets based on an assessment perceived or potential:

- Harm to Operations
  - Inability to perform current missions/business functions
    - In a sufficiently timely manner
    - With sufficient confidence and/or correctness
    - Within planned resource constraints
  - Inability, or limited ability, to perform missions/business functions in the future
  - Inability to restore missions/business functions
    - In a sufficiently timely manner
    - With sufficient confidence and/or correctness
    - Within planned resource constraints
  - Harms (e.g., financial costs, sanctions) due to noncompliance
    - With applicable laws or regulations
    - With contractual requirements or other requirements in other binding agreements (e.g., liability)
    - Direct financial costs
  - Relational harms
    - Damage to trust relationships
    - Damage to image or reputation (and hence future or potential trust relationships).
- Harm to Assets
  - Damage to or loss of physical facilities
  - Damage to or loss of information systems or networks
  - Damage to or loss of information technology or equipment
  - Damage to or loss of component parts or supplies
  - Damage to or loss of information assets
  - Loss of intellectual property
- Harm to Individuals
  - Injury or loss of life
  - Physical or psychological mistreatment
  - Identity theft
  - Loss of Personally Identifiable Information
  - Damage to image or reputation
- Harm to Other Organizations
  - Harms (e.g., financial costs, sanctions) due to noncompliance
    - With applicable laws or regulations
    - With contractual requirements or other requirements in other binding agreements
  - Direct financial costs
  - Relational harms
    - Damage to trust relationships
    - Damage to reputation (and hence future or potential trust relationships)
- Harm to the Nation



- Damage to or incapacitation of a critical infrastructure sector
- Loss of government continuity of operations
- Relational harms
  - Damage to trust relationships with other governments or with nongovernmental entities
  - Damage to national reputation (and hence future or potential trust relationships)
  - Damage to current or future ability to achieve national objectives
  - Harm to national security.

Finally, *NERC CIP-002-3* provides a classification approach that designates assets based on information compromise criticality; either – public, restricted, confidential, or private – suggesting that the level of security protection and controls can be managed by assignment commensurate with the risk of release.

**Public** - This information is in the public domain and does not require any special protection. For instance, the address and phone number of the headquarters of your electric cooperative is likely to be public information.

**Restricted** - This information is generally restricted to all or only some employees in your organization, and its release has the potential of having negative consequences on your organization’s business mission or security posture. Examples of this information may include:

- Operational procedures
- Network topology or similar diagrams
- Equipment layouts of critical cyber assets
- Floor plans of computing centers that contain critical cyber assets

**Confidential** - Disclosure of this information carries a strong possibility of undermining your organization’s business mission or security posture. Examples of this information may include:

- Security configuration information
- Authentication and authorization information
- Private encryption keys
- Disaster recovery plans
- Incident response plans

**Personally Identifying Information (PII)** - PII is a subset of confidential information that uniquely identifies the private information of a person. This information may include a combination of the person’s name and social security number, person’s name and credit card number, and so on. PII can identify or locate a living person. Such data has the potential to harm the person if it is lost or inappropriately disclosed. It is essential to safeguard PII against loss, unauthorized destruction, or unauthorized access.

## Cybersecurity Challenges

***Protecting Your Transportation Management Center*** (Fok, ITE Journal, February 2015) posed the following questions: What would happen if the United States could not...

1. Safely operate the transportation infrastructure for all modes?
2. Efficiently operate the systems to facilitate movement of people, goods, and services?
3. Communicate with the public for the public's interest and safety?

These three questions represent the penultimate risk question for today's surface transportation organizations. The purposeful inclusion of information technology assets to the already extensive list of what must be protected becomes a vital aspect of ensuring that the nation's transportation infrastructure can accomplish its mission and objectives.

## Chapter 3 Cybersecurity Plans and Strategies, Establishing Priorities, Organizing Roles and Responsibilities

### Security Planning

Security planning directs a transportation agency towards prevention and mitigation of the effects of security incidents by integrating those approaches that have proven to be successful into the operating environment. Development of a security plan provides an effective means to meet cost-benefit and competitive resource challenges. The plan can also reduce litigation risk and insurance costs. When the security plan is well structured and soundly developed using the appropriate strategies and elements, the resulting product can be a blueprint for short term and multi-year security planning. Security planning also sets out the policies and procedures related to security and any special requirements or considerations that are unique to the specific transit agency or state DOT.

*A security plan is a written document containing information about an organization's security policies, procedures, and countermeasures. The plan should include a concise statement of purpose and clear instructions about the agency security requirements... Creating a sound security plan is often as much a management issues as it is a technical one – It involves motivating and education managers and employees to understand the need for security and their role in developing and implementing an effective and workable security process. Organizational leaders must ensure that security planning is an actual functional activity and part of the agency's culture.*

*NCHRP Report 525 Vol 14, Security 101: A Physical Security Primer for Transportation Agencies*

The objective of security planning is to ensure both the integrity of operations and the security of assets. Transportation agencies already have planning processes and plans that address critical infrastructure protection and resilience, continuity of operations and operational issues such as incident management, equipment failures and other natural or accidental event. Planning for cybersecurity should result in the integration of security systems and processes into an agency's existing planning processes and daily business routine. This section includes an overview of planning recommendations, guidance for specific types of plans (cyber incident response plans, recovery plans) and a summary of recommended strategies to address cybersecurity of transportation systems.

Cybersecurity is not different than physical (or any other type of) security in that is an on-going effort that involves people and processes along with technology. Agency people – management, staff, contractors, vendors, etc. – must be aware of the need for security and educated on the security policies and procedures in place in the agency. The agency security strategy must be supported with specific policies and procedures tied to a matching organizational structure.

APTA, in *Recommended Practices for Control and Communications Systems*, recognizes cybersecurity as a process that should be incorporated into the transportation agency culture.

*Just as transit agencies have created a safety-centric culture—saving lives and reducing accidents and accident severity—they need to foster and create a cybersecurity culture. This requires an awareness program; a training program; an assessment of cybersecurity threats; a reduction of the attack surface (the number of places and ways someone can attack transit systems); a cybersecurity program that addresses: threats, mitigations, the software/firmware update process, monitoring and detection methodologies; and the ability to be audited to check for compliance via logs and change-management systems.*

***APTA Recommended Practices, Part 2***

Cybersecurity planning should incorporate, at the minimum:

- Security strategy that expresses management’s commitment to cybersecurity and provides the high-level direction and requirements for cybersecurity in the agency.
- Security policies that address the range of management, personnel, operational and technical issues and guide the development, implementation and enforcement of the agency security measures.
- Roles and responsibilities that clarify decision- making authority and responsibility for cybersecurity.
- Vulnerability and risk assessments to identify the agency-specific security requirements and assist in prioritization of risk management efforts.
- Development and Maintenance of cybersecurity plans including Risk Mitigation/Management and Response/Recovery plans.
- Active monitoring and evaluation on a continuous basis.
- Awareness and Training for all agency employees.

When planning for cybersecurity, some principles should be kept in mind:

- Address cybersecurity planning in a systematic way, with a commitment to a process of continuous improvement. Even with unlimited resources, it is not possible to eliminate all vulnerabilities and risks. Take a balanced approach that focuses on standards and incorporates learning from experience.
- Any cybersecurity program should be approached using risk management practices as a guide. Evaluate the agency’s specific cyber risks and develop the cybersecurity plan around managing those risks.
- An organizations security policy and controls must be adaptable to emerging threats in a constantly evolving world. Vulnerabilities are evolving and new risks are growing by the hour. Maintain situational awareness of cyber threats – both intentional and unintentional  
– as part of the plan.
- Failure will happen so it is important to plan for it, isolate it, contain its damage and recover from it gracefully. It is important to recognize that perfect security is not possible and that everything cannot be mastered. Planning ahead – having a Cyber Response and Recovery Plan - can ensure less damage from an incident.

Guidance exists for general cybersecurity plans, e.g. *NIST SP 800* series. However, to date, no comprehensive guidance has been developed to provide support for a transportation agency cybersecurity plan. *The Roadmap to Secure Control Systems in the Transportation Sector* (DHS, 2012) was developed to assist transportation agencies develop plans and the culture needed to sustain those plans. Guidance tailored for other sectors (e.g. nuclear, electrical and water) also has relevance for the transportation sector.

### **APTA Recommended Security Program**

APTA *Recommended Practice Securing Control and Communications Systems in Rail Transit Environments, Part 1* presents a four-phase transit control and communications systems security program which helps transit agencies manage cyber risk of those systems. The goal of a security program – one part of a security plan - is to identify risks and understand their likelihood and impact on the transportation system, put in place security controls (or countermeasures) that mitigate the risks to a level acceptable to the agency; and have in place response and recovery plans to minimize the impact of incidents and reduce the time to needed to get the system back to normal operations.

The overall recommendations developed by the APTA are based on NIST standards (i.e. *SP 800-18, SP 800-53*) and presents a four-phase control and communications systems security program to manage the cyber risk of those systems. The goal of the security program is to identify risks and understand their likelihood and impact on the transportation system, put in place security controls (or countermeasures) that mitigate the risks to a level acceptable to the agency; and have in place response and recovery plans to minimize the impact of incidents and reduce the time to needed to get the system back to normal operations.

Plan implementation requires support from senior management, system users, maintenance personnel, support staff, and system and equipment vendors. The four phases of the security program are:

- Phase 1 – Security plan awareness, establishment of a security team and risk assessment funding
- Phase 2 – Risk assessment and security plan funding
- Phase 3 – Security plan development and security countermeasures
- Phase 4 – Implementation of security plan measures and maintenance plan

#### **Phase 1**

Phase 1 requires management to understand the importance of cybersecurity countermeasures and the implications of a security breach within a transit environment. Senior managers establish the “tone at the Top” and lead by example to demonstrate the importance of cybersecurity to the agency and to foster a healthy respect for the programs and process put in place to support security. The senior managers establish the business objectives for security and the organizational roles/responsibilities. They provide the needed support - awareness, training and funding - for the organization’s security program. The leadership establishes and maintains the organizational “attention span” for cybersecurity.

In order for this to take place, senior managers must first understand why cybersecurity

is necessary. Technical personnel must explain to senior management the various impacts of a breach on life safety, equipment safety, revenue service, customer service and satisfaction.

Key activities based on best practices for this phase include:

- Ensuring active executive sponsorship for each stage of planning, deploying and monitoring cybersecurity efforts, which is critical to success of the efforts. Executive management will set the security objectives and align the strategic risk management with overall agency needs.
- Assigning responsibility for cybersecurity risk management to a senior manager so that risk mitigation, resource allocation decisions and policy enforcement all roll up to a clearly defined executive with the requisite authority.
- Defining the system(s) and critical cyber assets that need to be secured along with their classification (e.g. operational systems, payment systems, confidential information, PII, etc.) to assist in making informed decisions about risk severity and impact to the agency

## **Phase 2**

Phase 2 focuses on Risk Assessment of both physical and cyber elements to identify vulnerabilities and the likelihood of a loss of functionality due to system and/or component failure. The end state, as described in the *Transportation Roadmap (2012)* is “a robust portfolio of ICS-recommended security measures and analysis tools to effectively assess and monitor ICS cybersecurity risk.”

An important part of this phase is the risk assessment process, which was discussed in detail in the previous chapter. APTA recommends that this stage of the process include the following:

1. Generate management support and empowerment for the risk-assessment process.
2. Form the risk assessment team from technical experts and stakeholders.
3. Identify assets and loss impacts.
4. Identify threats to assets.
5. Identify and analyze vulnerabilities.
6. Assess risk and determine priorities for the protection of critical assets.
7. Identify countermeasures, their costs and trade-offs.

The assessment will involve the identification of all systems and assets and location of the equipment; access points that require cybersecurity; and users and their access levels/points. In addition, the Risk Assessment determines and quantifies the consequences of the loss of functionality and recommendations for the mitigation of the risks. The likelihood of functionality loss will be determined by system analysis and assessing the impact of failure (e.g., monetary, operations, life safety, infrastructure, equipment) for each component (hardware or system link). Ensuring that cybersecurity risks are incorporated in the agency’s overall risk management process is key. Identifying vulnerability and responding adequately to cybersecurity risks is not about knowing where cybersecurity can be improved, but knowing where it meets the level of collectively acceptable risk for a program, agency, organization, or region.

In addition to *APTA Recommended Practice, Part 1 and Part 2*, sources of information on

understanding cybersecurity risk and risk management include the *NIST Cybersecurity Framework*, *NIST SP 800-39 on Managing Information Security Risk*, *NIST SP 800-100 Information Security Handbook: A Guide for Managers*, *DHS USCERT's Risk Management/CEO Recommended Practices*, *DHS USCERT's Guide on CEO Questions to Ask*, and the *Guide to Developing a Cybersecurity and Risk Mitigation Plan*.

### Phase 3

Phase 3 is the development of the security plan and cyber and physical security countermeasures for new and existing systems and equipment. The plan should also cover equipment maintenance and support issues. APTA recommends that the security plan should contain the following elements: Control and communications systems boundaries:

- Identify the systems.
- Identify the equipment.
- Identify the locations.
- Identify the stakeholders.

Work group:

- Include all stakeholders.
- Identify responsibilities of the stakeholders.

Policies and procedures:

- Administrative
- Technical
- Cyber
- Physical
- Maintenance

Security measures:

- Management reports
- Maintenance issues
- Training

### Phase 4

Phase 4 is the implementation of the security plan through the establishment of a security plan management system and a maintenance plan. Much of this Phase will be described in *APTA Recommended Practice, Part 3*. Part 3 will continue to address security zones and introduce Attack Modeling for rail transit.

## ***Establishing Priorities***

### **NIST Cybersecurity Framework**

To assist in implementing an approach that is focused on standards, the National Institutes of Standards and Technology (NIST), working with industry groups and the private sector, has developed a framework of baseline standards for cybersecurity. The *NIST Cybersecurity Framework*, as called for in *Executive Order 13636*, in February 2014 to assist organizations in managing their cybersecurity risk.

*With an understanding of risk tolerance, organizations can prioritize cybersecurity*

activities, enabling organizations to make informed decisions about cybersecurity expenditures. Implementation of risk management programs offers organizations the ability to quantify and communicate adjustments to their cybersecurity programs. Organizations may choose to handle risk in different ways, including mitigating the risk, transferring the risk, avoiding the risk, or accepting the risk, depending on the potential impact to the delivery of critical services. The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management for the IT and ICS environments.

The NIST Framework is technology neutral and relies on existing standards, guidance, and best practice to provide “a common language for describing current and target states of security, identifying and prioritizing changes needed, assessing progress and fostering communications with stakeholders. It is meant to complement, not replace, existing cybersecurity programs”.

The Framework is designed to provide a common taxonomy and mechanism for organizations to:

- Describe their current cybersecurity posture;
- 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.

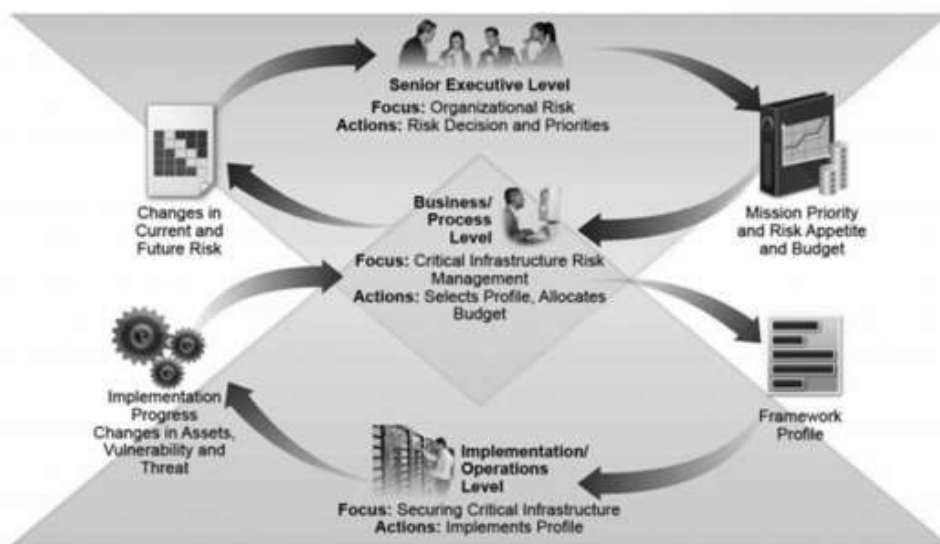


Figure 6: Cybersecurity Risk-Based Framework. Source: NIST Cybersecurity Framework, 2014.





**Figure 7: NIST Framework Implementation Steps. Adapted from Energy Sector Cybersecurity Framework Implementation Guidance, US Department of Energy 2015**

<b>Step</b>	<b>Inputs</b>	<b>Activities</b>	<b>Outcomes</b>
1	Risk management strategy Organizational objectives and priorities Threat information	Determine where to apply Framework to evaluate and guide cybersecurity capabilities	Scope of Framework in Organization
2	Risk management strategy Framework Scope	Identify in-scope systems and assets Identify standards, guidelines and tools	Systems & Assets Cybersecurity requirements & standards
3	Evaluation approach Systems and Assets Requirements and Standards	Identify current cybersecurity and risk management state	Current Profile
4	Risk management strategy Evaluation approach Systems and Assets Requirements and Standards	Perform risk assessment	Risk Assessment
5	Current Profile Organizational objectives Risk management strategy Risk assessment reports	Identify goals to mitigate risk consistent with organizational goals and critical infrastructure objectives	Target Profile
6	Current Profile Target Profile Organizational objectives Organizational constraints Risk management strategy Risk assessment	Analyze gaps between current and target profile Evaluate consequences from gaps Prioritize actions (cost-benefit analysis, consequences) Create action plan	Prioritized gaps Prioritized implementation plan

7	Prioritized implementation plan	Implement actions by priority Track progress against plan Monitor/evaluate progress against risks, metrics and performance indicators	Project tracking Data New security measures implemented
---	---------------------------------	---	--

### Case Study – Idaho Transportation Department (ITD)

The Idaho transportation department has jurisdictional responsibility for almost 5,000 miles of highway (or 12,000 lane miles), more than 1,700 bridges, and 30 recreational and emergency airstrips. ITD also has responsibility for the Department of Motor Vehicles (DMV) as one of DOT functions, with the resultant need to protect state residents PII found in driving permits, driver's licenses, and other related information. With a significant black market value for Social Security and driver's license numbers, this added incentives to the challenge of improving the cybersecurity of the agency.

ITD looked at frameworks and approaches to support their efforts. ISO standards were being used at the agency and the team reviewed SANS 20 guidance before deciding to utilize the NIST Framework. The NIST framework provided a common set of terms and values so that the agency could create metrics on movement towards goals - what investment looked like in terms of agency-specific goals and the work accomplished to address identified gaps. The framework gave the agency a structure for demonstrating ROI for the investment of resources, employees and tools that reduced the cyber risk of the agency.

To implement the framework at ITD, the agency needed to identify its cyber-related goals (the primary focus was security of DMV related information) and then do an internal analysis on where the current systems were in terms of recommended guidance. The agency went through each NIST framework function (identify, protect, detect, response, recover) by category and subcategory, to assess by tier - a scaled that ranged from partial, through risk informed, then repeatable to adaptive - where the agency's cybersecurity efforts currently were. ITD added a zero to the scale, recognizing that in some categories and subcategories, the agency either had not been aware, or may not have been addressing certain aspects of security.

Based on their experience, ITD recommends setting targets first before conducting the assessments. They caution about setting targets too high, which can result in high cybersecurity costs. Because the targets can be reset over time, the agency recommends focusing on agency-specific cybersecurity risks. For example, for securing customer information ITD considered each function category based on value he data. of data.

ITD found the one of the most difficult parts of the process was understanding how recommended cybersecurity and countermeasures guidance documents such as NIST SP 800 series documents applied to a transportation agency since some were initially geared to federal agencies to address FIPS compliance. It was a challenge to ITD team doing work, but the results were worth it. ITD forced to take hard look at their systems and current approaches and to ask hard questions, especially in deciding how to score the agency. They had to decide on

agency goals, which forced them to take a holistic view of whole program.

The NIST Framework does not include metric charts and graphical representation in the guidance, so what ITD developed their own to use. They wanted to create metrics to represent in graphical format what investment looked like, e.g. how the agency was moving toward the goals. The agency created a chart that summarized the tier assessments by function and that information is presented to leadership on a regular basis. The figure below provides an illustration used by ITD with quarterly results. Goals have been set for each function based on the priorities set by the agency. ITD found that over time, as it became more cybersecurity-adept, the scoring became "harsher" than the initial assessment over time, so in some instances the tier was less in a subsequent quarter. Note: Other organizations have created metrics adapted NIST Framework to easily convey to management their risk treatment plan and results. University of Michigan utilizes a hi/med/low rating instead of the scoring system used by Idaho.

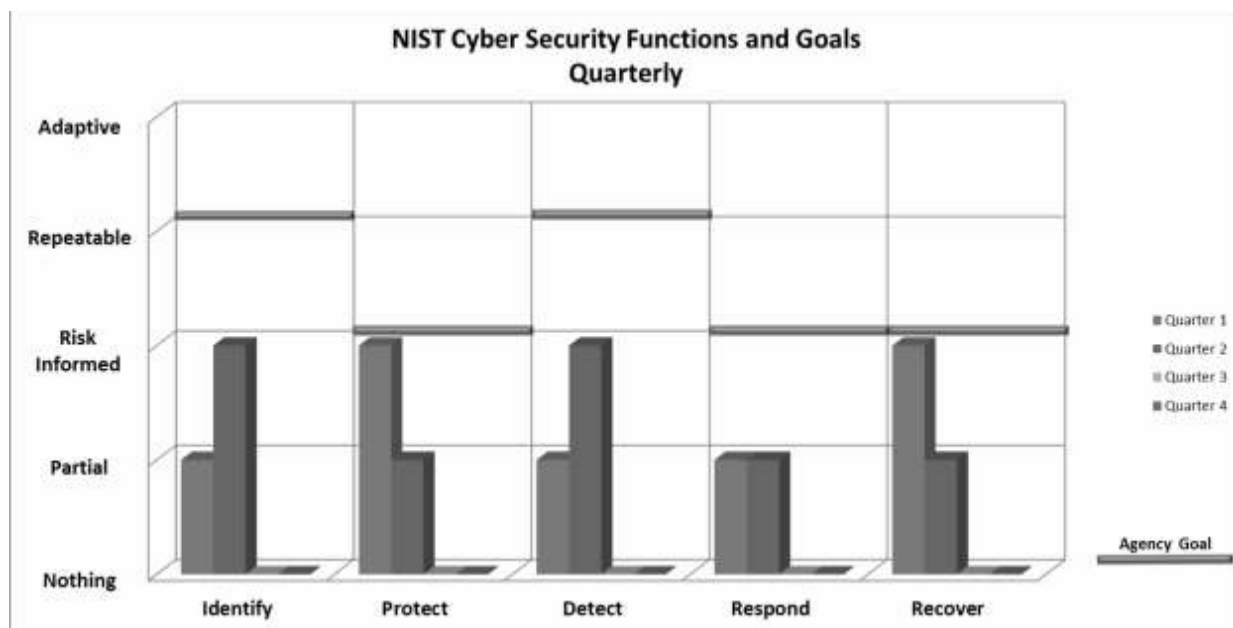


Figure 8: Example of ITD NIST Framework Quarterly Goal Tracking

The process allowed the IDT team to successfully address the cybersecurity funding challenges of how much budget is available and where in the agency does the budget come. Initially, there was a one person cybersecurity team with tools being paid from business area budgets. Using the NIST framework and the graphic 'results' chart, support from senior management was easier to obtain. The chart provided a way to show the agency cyber risk as part of a holistic, 'big picture' and could demonstrate the ROI - making the DOT more secure.

### ***Defense in Depth Approach***

Defense-in-Depth Strategy is a high-level recommended approach for cybersecurity countermeasures. The approach involves multiple layers of defenses protecting critical assets and systems. The approach does not focus on a few countermeasures but a range of

them from perimeter defense to policy and procedures to training and awareness. The figure below presents the Defense in Depth strategic framework. Defense in Depth was created by the NSA and has been adopted as a recommended practice by the DHS-CSSP. APTA has adopted this strategy for the protection of rail transit communications and control systems.

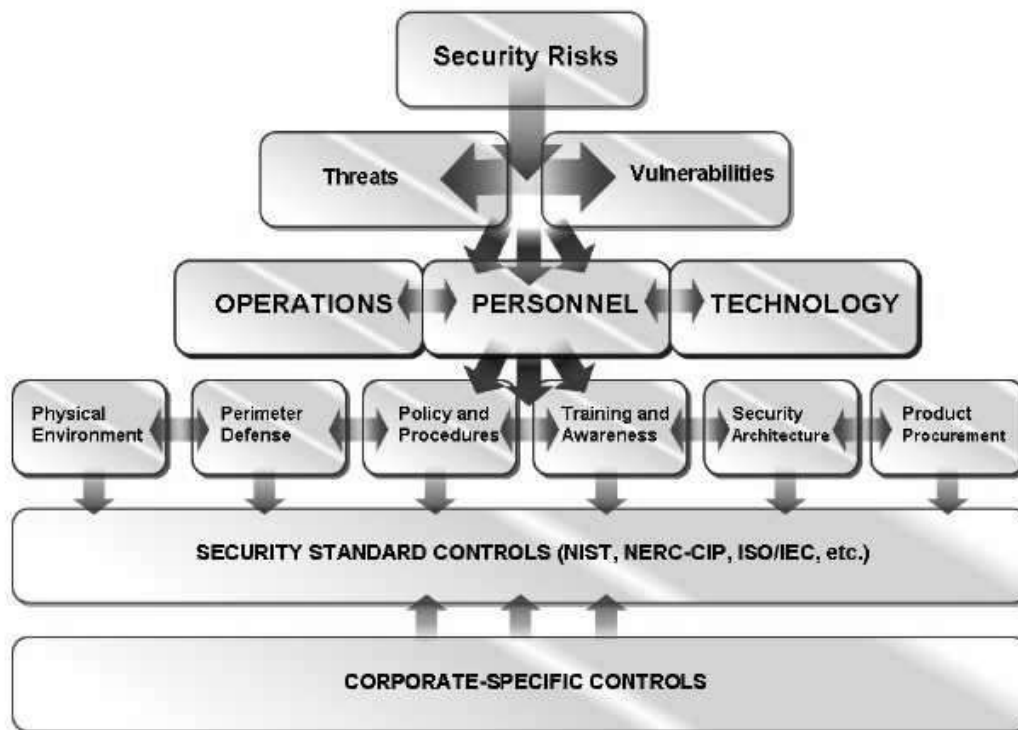


Figure 9: Cyber Defense-in-Depth Strategic Framework

Source: DHS Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, 2009

A Defense in Depth strategy begins with understanding and measuring the risks faced by the agency, using resources to mitigate the risks, identifying overlapping areas of core competencies of resources, using appropriate security standards and customizing or creating specific controls for the agency. The strategy is based on having the aggregate of all security activities provide complete protection for an organization's ICS. (*DHS Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, 2009*)

This strategy promotes cybersecurity through:

*“increasing the amount of time and number of exploits needed to successfully compromise a system; increasing the likelihood of detecting and blocking attacks; allowing security policies and procedures to better align with agency organizational structure; and directly supporting the identification and implementation of cybersecurity risk (or impact) zones.” (APTA Recommended Practice Part 2)*

A key aspect of the strategy is the division of systems architecture into zones with each zone having its own defensive strategy and monitoring and securing zone boundaries and any necessary connections among zones. Zones are identified based on security requirements and

may be one of two types of zones – architectural or risk zone. Architectural zones are physically distinct areas managed by separate business units. Risk zones or impact zones group functions based on impact type and may be under the purview of more than one business unit. The example provided by DHS in the *Recommended Practice (2009)* is a Zone Model for Manufacturing. The Model contains five zones: external, corporate, manufacturing/data, control/cell, and safety; each zone is prioritized according to security requirements.

Specific aspects of the strategy include the following:

- Develop ICS-specific security policies, procedures, training and educational content and address security throughout the ICS lifecycle
- Align ICS security policies and procedures with threat level
- Separate ICS and corporate networks by using appropriate network architecture and providing logical separation.
- Ensure availability by implementing redundant critical components (or networks) and designing fault tolerant critical systems to avoid cascading events
- Restrict physical and virtual access through separate authentication for ICS and corporate networks, and user privileges should be based on the principle of least privilege.
- Prevent, deter, detect, and mitigate introduction, exposure, and propagation of malware through security controls, security patches, and disabling unused ports and services after testing; and tracking and monitoring audit trails to detect patterns and identify vulnerabilities
- Zones – a key aspect of the strategy is the division of systems architecture into zones with each zone having its own defensive strategy and monitoring and securing zone boundaries and any necessary connections among zones. Zones should be identified based on security requirements. There are two types of zones – architectural and risk zones. Architectural zones are physically distinct areas managed by separate business units. Risk zones or impact zones group functions based on impact type. Risk zones may be under the purview of more than one business unit. (The example provided by DHS is a Zone Model for Manufacturing. The Model contains five zones: external, corporate, manufacturing/data, control/cell, and safety; each zone is prioritized according to security requirements.)

It should be noted that Defense-in-Depth does not eliminate all vulnerabilities and risks in a system. Recent research (Firefly, 2014) found that 97% of systems utilizing a Defense-in-Depth approach were still found to have been compromised.

### **Security Zones Approach**

With limited resources and budgets, it is impossible to protect all systems and apply all recommended countermeasures and approaches to the fullest extent. To address this reality, taking a zoned approach can help in the prioritization of efforts.

APTA Recommended Practice defines security zone classifications and recommends minimum set of security controls for most critical zones. To implement this approach, it is important for an agency to identify and place its functions/systems in a series of security zones. The following are the three security zones identified by the APTA CCSWG in *APTA Recommended Practice, Part 2*, presented in increasing level of safety criticality:

- Operationally Critical Security Zone (OCSZ) – This is the control center zone and includes the SCADA, train control, traction power, dispatch, passenger information system and associated equipment.
- Fire, Life-Safety Security Zone (FLSZ) – The systems in this zone warn, protect or inform in an emergency. Systems include emergency management panels, emergency ventilation systems, fire detection and suppression systems, and traction power emergency shutdown systems.
- Safety Critical Security Zone (SCSZ) – The systems in this zone are those that if modified can present immediate threat to life or safety. Vital signaling, interlocking and ATP are examples of such systems.

There are two additional zones associated more with IT than with control systems the Enterprise Zone which includes accounting systems and schedule systems and the External Zone which includes communications with the internet and vendors.

**Table 1: APTA Cybersecurity Zones**

Importance	Zone	Example System
Most Critical	Safety Critical Security	Field signaling
	Fire, Life-Safety Security	Fire Detection/suppression
	Operationally Critical	Traffic Management
	Enterprise	HR, Accounting
Most Public	External	Communications with public, vendors, others

The model security zone chart in Figure below depicts the location of these zones in different areas of the rail transit system.

## Model Control & Communication System Categories



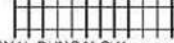















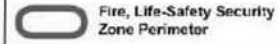

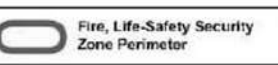
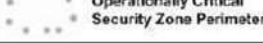
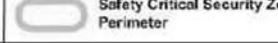
EXTERNAL ZONE:	<input type="checkbox"/> VPN to other Vendors <input type="checkbox"/> VPN to other Agencies	<input type="checkbox"/> N/A	<input type="checkbox"/> N/A
 OCC	 Train station / Station Equipment Room	 SIGNAL BUNGALOW – or equivalent	
 <input type="checkbox"/> Access Control System <input type="checkbox"/> Advertising <input type="checkbox"/> Fare Sales / Collection <input type="checkbox"/> Credit Card Processing <input type="checkbox"/> Logging	 <input type="checkbox"/> Access Control / Intrusion Detection <input type="checkbox"/> Advertising <input type="checkbox"/> Fare Sales / Collection <input type="checkbox"/> Passenger information system <input type="checkbox"/> CCTV	 <input type="checkbox"/> N/A	
 <input type="checkbox"/> Dispatch / ATS <input type="checkbox"/> Non-Emergency Voice Communications <input type="checkbox"/> SCADA	 <input type="checkbox"/> Traction Power <input type="checkbox"/> PA System – Passenger Information Display <input type="checkbox"/> Vertical Lift Devices <input type="checkbox"/> Tunnel pumping / draining	 <input type="checkbox"/> Traffic Controller Interface	
 <input type="checkbox"/> Emergency Communications <input type="checkbox"/> Fire Alarm & Suppression Enunciators <input type="checkbox"/> Fire / Life-Safety, Emergency Ventilation Control <input type="checkbox"/> Status displays	 <input type="checkbox"/> Emergency Ventilation Systems <input type="checkbox"/> Emergency Management Panel <input type="checkbox"/> Fire Detectors / Alarms / Suppression systems <input type="checkbox"/> Safety Critical Physical Intrusion Detection <input type="checkbox"/> Traction Power Emergency Cutoff <input type="checkbox"/> Traction Power Protection Relaying <input type="checkbox"/> Gas Detection <input type="checkbox"/> Mass Notification PA <input type="checkbox"/> Seismic Monitoring	 <input type="checkbox"/> Safety Critical Physical Intrusion Detection	
 <input type="checkbox"/> Vital CBTC	 <input type="checkbox"/> Vital Signaling, ATP <input type="checkbox"/> Platform Gate Control	 <input type="checkbox"/> Vital Signaling, ATP <input type="checkbox"/> Crossing Gates	
<b>LEGEND</b>  Enterprise Network (Admin, IT, HR)  Fire, Life-Safety Security Zone		<b>LEGEND</b>  Enterprise Zone Perimeter  Fire, Life-Safety Security Zone Perimeter	
 Operationaly Critical Security Zone (Traction Power)  Safety Critical Security Zone		 Operationaly Critical Security Zone Perimeter  Safety Critical Security Zone Perimeter	

Figure 10: Model Control & Communications System Categories Source: APTA Recommended Practices, Part 2

*APTA Recommended Practices Part 2* recommends combining Defense in Depth with Detection in Depth. Detection in Depth detects intruders and implements detection for each zone and layer. It is based on the concept of least privilege, which initially restricts all outbound traffic and subsequently permits only necessary outbound connections.

To assist transit agencies in implementing the approach, an example transit system shown in the Figure below provided in *APTA Recommended Practice, Part 2*. The model transit system has seven stations, two lines, passengers, vendors, and staff; the staff is divided into various groups such as the signals and communications group, track maintenance, fire response, life safety and the operations group.

## Example Transit System – Rail – Fixed-Block Signaling

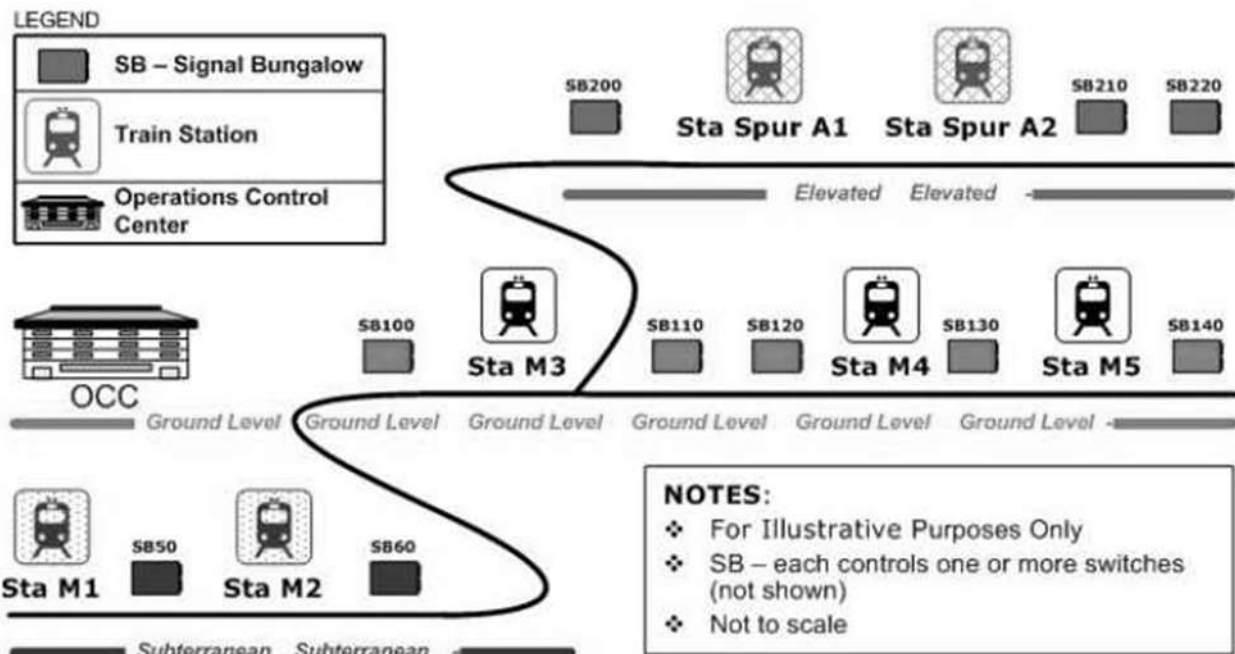


Figure 11: Model Transit System. Source: Figure 5, APTA Recommended Practice, Part 2

### Attack Modeling

*APTA Recommended Practice Part IIIa* recommends Attack Modeling Security Analysis as a countermeasure for large or complex projects including upgrades and installation of new technologies.

Attack modeling involves the creation of attack trees which depict the series of steps needed for an attack to transpire or a system to become compromised. Attack modeling is formally defined as:

*“[A] method of detailed security analysis of a control and communications system considering a range of threats and in what ways a system may be attacked. By studying the pathways through which an attack may be carried out, a relative ranking of the risks of system compromise from these threats may be compiled and countermeasures planned to prevent these attacks.” (APTA Part IIIa)*

Commercial and open source attack modeling software is available to support the analysis process and develop the attack trees.

The attack modeling process involves the following steps:

1. Characterize the system
2. Describe normal sequence of operations, along with data flows
3. Decompose operations into sequence diagrams
4. Identify threats to system during operating sequences
5. Build attack trees



6. Decision point: evaluation type (short or long method)
7. Use the Short Method or Long Method

A Case Study of a hypothetical U.S. transit agency with a conventional fixed-block signaling system is provided in Section 4 of APTA Part IIIa.

### ***Organizing Roles and Responsibilities***

Understanding and defining the roles and accountabilities of the organization's functions and employees in support of the agency's security mission and operations are critical. However, it is important to be realistic in what can be supported by the engineering and operational team, the IT support team, and vendors by understanding the technical, legal, and institutional limits under which the support team is operating.

It is critical to facilitate discussion and interaction between the IT, engineering and operational groups. Cybersecurity is generally the responsibility of IT personnel. Control systems are usually the responsibility of engineering and operations personnel. Implementing cybersecurity for transportation control systems requires having a good understanding of security AND the controls systems and the operational environments.

Utah Transit Agency (UTA) has instituted a cybersecurity program that includes integration of employee training, established governance and procedures, and technical solutions. The agency has established cybersecurity support process that reduces the culture "gap" between IT and operations. Cross-training of transit operational staff with IT was conducted instituted on cybersecurity to allow improved communications and interactions between the divisions. IT staff understood that the 'T' in UTA stood for "transit" not "technology".

Some cyber incidents may require outside support. Very few transportation agencies have the expertise and skills to respond to every cyber incident. Including in the risk matrix what risks are manageable by local staff and which ones are not, and understanding when the limit is reached and where to get help is important. The U.S. Department of Transportation (USDOT) developed a Cybersecurity Action Team to support the Incident Response Capability Program.

### ***Relationship with Physical Security***

Cybersecurity cannot be easily separated from physical security. Inadequate physical security can put cyber assets in jeopardy. Physical damage can compromise cyber assets. Evidence of intrusion into physical assets, especially control system cabinets, devices or terminals, communications devices or networks, is an indicator for a suspected cyber breach. Along with more obvious damage or telltale evidence of intrusion and unreconciled door and/or cabinet alarms, inexplicable loss or behavior of communications links or behavior of control system devices could be indications of physical security breaches. Policies and practices for responding to physical security breaches need to also address cybersecurity, and incorporate considerations that a cyber-related incident may have also occurred.

*ICS Cybersecurity Response to Physical Breaches of Unmanned Critical Infrastructure Sites (SANS Analyst Whitepaper, ICS-CERT, 2014)* provides recommendations for responses to physical breaches with potential cybersecurity impacts. (*NCHRP Report 525 Surface Transportation Security, Volume 14 Security 101: A Physical Security Primer for Transportation Agencies* provides additional information and resources on physical security of transportation systems.)

SANS/ICS CERT recommends a three level cyber response approach after conducting a physical examination of the location for anything that appears to be missing or out of place. The three levels are:

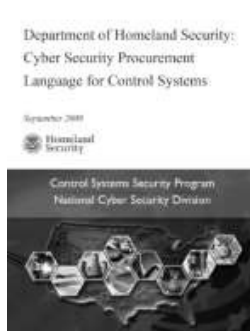
1. **Initial physical examination** to assess physical connections, evidence of tampering, alarm status/indicators and unfamiliar or new hardware or media (e.g. USB devices, wireless cards, access points or any other cover hardware devices used to compromise cyber systems).
2. **Systems and configuration checks** to identify forensic evidence of intrusions such as new user accounts, hidden files, unauthorized configuration changes, and unusual network activity.
3. **Detailed examination of files system and binaries**, if necessary, to confirm files are clean and uncorrupted, proper configuration of network devices, and no evidence of unauthorized firmware updates.

Each level in the response approach requires more technical and operational expertise and closer coordination between the cybersecurity experts and the operational engineers. Along with the skills and of hardware and software installation for the potentially impacted control systems, the appropriate vendors and consultants may need to be involved with the in-house technicians.

### Procurement Language Guidance for Vendor Contracts

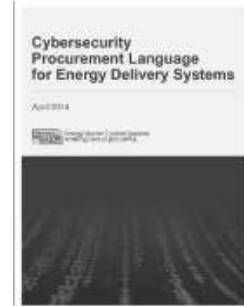
Recognizing that cyber systems are often purchased from vendor and not always developed in-house, the U.S. Department of Homeland Security (DHS) worked with industry cybersecurity and control system subject matter experts and the U.S. Department of Energy (DOE) to produce *Cybersecurity Procurement Language for Control Systems*, published in 2009.

The document summarizes security principles that should be considered when designing and procuring control systems products and services (software, systems, maintenance, and networks), and provides examples of procurement language text mapped directly to vulnerabilities of control systems to incorporate into procurement specifications. Created in a process that brought together leading control system security experts, purchasers, integrators, and technology providers and vendors across many industry sectors (e.g., electricity, natural gas, petroleum and oil, water, transportation, and chemical), the guidance was designed to assist both system owners and integrators in establishing sufficient control systems security controls within contract relationships to ensure an acceptable level of risk.



The NIST *Framework for Improving Critical Infrastructure Cybersecurity*, in identifying a common language to address and manage cybersecurity risk, provides a language that may be leveraged in the procurement process – it can be used as a tool to help communicate cybersecurity requirements in the procurement process.

The energy sector cybersecurity working group (ESCSWG) - a public-private partnership consisting of asset owners, operators, and government agencies – using the 2009 DHS documents as a foundation developed a baseline cybersecurity procurement language guidance document, *Cybersecurity Procurement Language for Energy Delivery System (2014)*, guided by the NIST Framework. Although it was tailored to the specific needs of the energy sector, the suggested procurement language has relevance for all sectors including transportation.



It should be noted that both the DHS and the ESCWG documents focused on the cybersecurity of control systems and did not address cybersecurity-based procurement language for IT. Recommendations for IT cybersecurity procurement are included in the NIST 800 series of publications and other standards and guidance documents.

The 2014 energy sector provides baseline cybersecurity procurement language for individual components (e.g., programmable logic controllers, digital relays, or remote terminal units) and individual systems (e.g., a SCADA system, EMS, or DCS). It also “*differentiates the cybersecurity-based procurement language that is common to the procurement of individual components and systems from language that is only applicable to individual components or systems. Furthermore, this document differentiates language that is applicable to specific technologies (e.g., Transmission Control Protocol/Internet Protocol [TCP/IP] communication between systems or components, and remote access capabilities)*”.

There is a section that provides general cybersecurity considerations that apply to many types of products being procured grouped into the following topic areas:

- Software and Services
- Access Control
- Account Management
- Session Management
- Authentication/Password Policy and Management
- Logging and Auditing
- Communication Restrictions
- Malware Detection and Protection
- Reliability and Adherence to Standards

A number of procurement language elements presented request summary documentation or verification from the Supplier. For example:

*The Supplier shall provide summary documentation of procured product’s security features and security-focused instructions on product maintenance, support, and*

*reconfiguration of default settings.*

Another example:

*The Supplier shall provide a method to restrict communication traffic between different network security zones. The Supplier shall provide documentation on any method or equipment used to restrict communication traffic.*

Additional sections provide language to consider when acquiring intrusion detection systems, focused on physical security considerations and wireless technologies, and on cryptographic technology.

As noted in both of the resources cited above, the procurement language presented in the documents is not all-inclusive. Depending on the product and services required by the transportation agency, additional cybersecurity-based procurement language beyond what has been identified in these documents may be necessary.

In addition, as the cybersecurity landscape continues to evolve, new threats, technologies, techniques, practices, and requirements may need to be considered during the procurement process. The procurement language will need to evolve to meet the challenges of this changing landscape.

## Chapter 4 Transportation Operations Cyber Systems

### *Introduction*

Along with other sectors of the nation's critical infrastructure, over the past three decades the surface transportation sector has gradually added various operations technologies that augment – and in many cases interoperate with – existing back office enterprise data systems and also newer customer-focused internet applications. Some of these technologies, such as rail crossing signals, were adapted from earlier Industrial Control System (ICS) architectures; others, such as vehicle location and tracking, grew from other roots and are unique to transportation. Although the trend in automating transportation control processes has been most accelerated in public transportation (i.e., transit) operations, recent initiatives in the highway operations arena highlight the challenges of maintaining adequate levels of cybersecurity in this area, as well.

Although the scope of this Primer encompasses those activities involved with operating all components of the surface transportation infrastructure, the differences between the technologies typically used in highway, public transportation and railroad operations are significant enough to view them as largely distinct subdomains. Similarly, while such diverse issues such as the threat space and attack surface; enterprise and information security architectures; personnel; facilities; supply chain relationships; organizational governance and culture; procurement and acquisition processes; organizational policies and procedures and many organizational assumptions facing transit operators and their highway manager counterparts may also be converging, significant differences still exist and this Chapter will discuss cybersecurity associated with each modality separately.

This Chapter introduces general concepts associated with this amalgamation of industrial control technologies, enterprise data management systems and traffic management technologies. The Chapter will describe essential differences between data-centric systems and control-centric ones. The Chapter will provide a brief overview of the types of systems used in infrastructure operations and potential cybersecurity issues associated with each. General and system specific countermeasures will be presented in the next Chapter.

Finally, the Chapter discusses recent and on-going national initiatives leading to standards and recommended practices.

### *Transportation Operations Cyber Systems*

A single transportation agency may own, operate and use hundreds of automated systems supporting all aspects of its transportation infrastructure management business (i.e., planning, engineering, construction/maintenance, operations, and business management). This technology portfolio contains a unique and constantly changing set of proprietary (i.e., custom built) plus commercial-off-the-shelf (COTS) software and hardware investments. Some agencies have made recent major investments in state-of-the art major upgrades or replacement systems; conversely, others still maintain technology assets (e.g., railroad crossing signals) that may be decades old.

This state of affairs leads to legacy systems in use today spanning over four generations of

computing architectures (i.e., mainframe, client/server, Web 1.0 to Web 4.0 and mobile) and at least two generations of control system architectures (i.e., analog and digital). As a consequence, most of the systems used in transportation are poorly integrated, barely interoperable and in many cases, technically incompatible both within and across subsystems, systems and organizational boundaries. Each of these technical architectures presents different operational characteristics and technical security challenges. Of specific importance, the modern security manager should be aware that for the most part, the legacy systems he or she inherits were not designed with cybersecurity in mind.

Legacy system governance (including security) models also encompass a wide spectrum of institutional oversight and control options ranging from highly centralized state-level or enterprise-wide structures at one end to those permissive of fragmented user autonomy (i.e., anarchy) at the other extreme. A common governance pattern found in many agencies assigns the responsibility for infrastructure control systems to the engineering operations group while assigning the responsibility for general computing and information security to an IT bureau usually located in the business management side of the organization. These two groups are far removed from each other in their respective chains-of-command, knowledge, skills and culture, often making communication and cooperation difficult. In many cases, governance alternatives to this *status quo* are strictly proscribed by a complex and unique set of Federal, State, local and agency-level regulations, policies and administrative procedures. Each of these governance approaches also results in different organizational and behavioral norms and leads to unique operational security challenges.

Until recently, most technology investment decisions were justified based solely on the effectiveness or efficiency impacts of that investment on a transportation service, product or business process. Cybersecurity was treated as a system externality and was generally not included in cost/benefit analysis, user needs or technical requirements pieces although recent highly publicized cyber incidents compromising commercial and consumer privacy and financial information have begun to change this practice, particularly in the government, banking and retail sectors.

Over the past generation, the clear trend in the surface transportation industry has been to rely on 3<sup>rd</sup> party technology partners (e.g., external IT agencies, vendors, manufacturers, consultants and system integrators) more interested in achieving contract-based performance metrics and maintaining profit margins than in maintaining cybersecurity. Indeed, in many cases, adding “aftermarket” cybersecurity components such as anti-virus software may invalidate warranties;

violate contractual provisions or negatively impact system performance. Consequently, the resultant transportation operations technology ecosystem itself places severe constraints on an individual agency’s ability to incorporate cybersecurity enhancements. *In other words, the system customer may not be able to implement necessary and foundational technology-based cybersecurity enhancements, in spite of their best intentions.*

These four aspects of transportation systems create the background against which the security manager must evaluate the best practice recommendations contained in this Primer.

1. Large, complex cyber asset bases.
2. Cumbersome and inflexible governance structures.
3. Incompatible mission requirements.
4. Security-agnostic technology ecosystem.

Two conclusions derived from this discussion offer essential cautions:

1. No “one-size-fits-all” cybersecurity program, technology or training exists or can ever be developed; each agency must determine, deploy and operate countermeasures unique to its local circumstance. These circumstances are continuously evolving forcing the continual evaluation and evolution of effective cybersecurity measures.
2. Although this Primer contains guidance on a variety of possible countermeasures, many recommended practices may be unavailable or not implementable due to local regulatory, governance, commercial, technical or other resource constraints.

### ***IT Systems used in Transportation Infrastructure Operations***

Most Information Technology (IT) used in transportation operations focuses on customer-centric data processing and as such, contains and communicates a wide variety of personally identifiable information (PII) - sensitive information about agency customers and employees such as name, SSN, address, credit card, insurance and banking details, driver’s license data, digital ID photo and more. Examples in the highway domain include driver licensing and vehicle registration systems, electronic toll collection and other use-permitting applications; several transit systems also maintain PII including fare sales and some rider alert systems.

Other IT or enterprise data systems used in both highways and transit agencies include general business administration systems (e.g., Financial systems including bidding, purchasing and supplies inventory systems and Human Resource systems including payroll and banking subsystems), asset management systems including asset location, condition and inventories and also asset engineering data including sensitive data such as engineering plans and inspection data.

The primary emphasis of information security as it relates to IT is the protection of information assets (i.e., data plus all associated information infrastructure) from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide:

- (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- (C) availability, which means ensuring timely and reliable access to and use of information. (*44 USC, Sec 3542 (b)(1)*)

Transportation organizations, as do many other public- and private-sector organizations, typically place a higher emphasis on the confidentiality and the integrity of their IT systems and data resources since the short-term disruption of data system availability at worst creates a delay in business operations and is not considered to be a threat to public or environmental health and safety. This assessment is generally made by the individual information system owner who, in most cases, is not the organization’s security officer. Moreover, this assessment is always made at the local level and is not determined through a uniform national consensus

process or required by regulation.

Loss of data confidentiality (i.e., cyber theft) was minimal (i.e., non-reported or not known to the agency), particularly due to the arcane, isolated nature of the technical architectures employed. The risk of cyber theft is increasing however as transportation data applications move to more open and accessible platforms and as the number of motivated and competent thieves increase. New Federal guidelines for the protection of PII resulting from the increasing level of highly publicized PII cyber theft (e.g., the Chase bank, Home Depot, Federal OPM and Target store breaches of 2014 and 2015) may have a significant impact on these systems and their users in the near future.

Emerging security issues in transportation IT include:

- “Bring your own Device”
- Customer self-service internet applications
- Technical interdependencies

These issues are expected to/will undoubtedly impact ICS security as increased integration of IT and ICS occurs and with the advent of hybrid ICS-IT systems.

### ***Industrial Control Systems used in Transportation Operations***

At the same time that the transportation industry was building IT systems, it was also automating many aspects of traffic, transit and related infrastructure operations. Beginning with the simple electro-mechanical devices of the early 20<sup>th</sup> century, the industry has installed billions of dollars of technology to monitor and control vehicles, operate signs, signals, gates, bells and warning lights; surveil traffic, inspect infrastructure, collect fares and tolls and control HVAC, lighting and fire alarm systems; and install operate and maintain other infrastructure devices, sensors and alarms. This combination of sensors, controllers, effectors and Human Machine Interfaces is collectively referred to as Industrial Control Systems (ICS). Over time the first generation of ICS devices were replaced by solid-state components which are now increasingly both digital and network connected. “Smart” meters, “smart” signs, “smart” phones and other smart devices with embedded processors and network connectivity are the order of the day.

Even as the underlying technical architectures of IT and ICS began to converge (and in many cases to be shared), the basic distinction between IT and ICS remains. Simply put for the purposes of this Primer: *IT systems manage data or information; ICS systems control the physical world.* Stated another way, if the end result of a user interaction is to add, update or delete data in a permanent record, file or database, the underlying technology is IT. On the other hand, if the end result of an interaction is to control one or more physical entities based on real-time environmental variables, the technology is ICS-based. Highway-rail grade crossing automated warning systems are ICS-type technology where trains approaching at-grade crossings will trip a train circuit, activating warning signals and crossing barriers and in some cases changing nearby traffic signals.

Of course, there are many hybrid systems which have both effects. For example, some Highway Road and Weather Systems (RWIS) not only activate warning signs and close access gates based on such variables as visibility but may also communicate status information to a traffic management center or to a 411 database. These systems may also generate and store



persistent data for subsequent post-storm analysis and modeling. Another hybrid application uses smartphones as smart keys working with smart locks installed in vehicles and buildings.

The Table below illustrates common examples of ICS and IT technology used in surface transportation.

**Table 2: Transportation Operations Systems**

Type	Category	Highways	Transit
Operational Systems	Control Systems	Advanced Traffic Management System (ATMS)	Train Control System Bus Control Systems
	SCADA	Road/Weather Systems Traffic Monitoring and Surveillance RR Crossings GPS	Traction Power Emergency Ventilation System Monitoring (Pumps, Alarms)
	Signaling	Highway Signals	Train Signals Signal Priority Systems
	Communications	Advance Traveler Information System (ATIS)	Communications DSRC
	Fare Collection Systems	Electronic Toll Collection (ETC)	Entry/Exit Gates Ticket Vending Machines, Fare Boxes, Fare Validators, Ticket Encoding
	HVAC/Building Management	HVAC Tunnel Ventilation	HVAC systems (not integral part, but loss could result in failure of critical systems) "People Movers"
Enterprise Data Systems	Business/Revenue/3 <sup>rd</sup> Party systems: Finance, HR, Messaging (email), Archives	Driver, Vehicle and Crash systems Asset Management BYOD	Asset Management BYOD
Engineering Systems	Design, Construction	CADD, Electronic Bidding	Track Inspection

Historically IT and ICS used separate and distinct architectures, hardware, software and communications components and protocols. Each technology was acquired and operated by different user groups with different backgrounds, training, and mission. This organizational and technical "air-gap" strategy essentially allowed these two domains to independently exist without any cross-domain interdependence or impacts.

However, over the past generation, ICS vendors/manufacturers began to incorporate IT protocols (e.g., Ethernet, IP, NTCIP), operating systems (OS) (e.g., MS Windows), and other low cost, widely available technologies (e.g., processors, routers and storage devices) replacing older proprietary components.

In addition, ICS systems used in transportation now routinely share enterprise IT solutions promoting network connectivity, data sharing and remote access capabilities. In extreme cases the same communication infrastructure carries voice traffic, along with enterprise data and control system signals. Other enterprise capabilities such as data archiving may also be shared between IT and ICS.

This convergence and connectivity of IT and ICS technologies has now created a situation where

- Newer ICS systems are beginning to converge with IT systems inheriting their vulnerabilities as well as their capabilities;
- ICSs are no longer technically obscure and isolated from the "outside world;"
- Interconnecting IT and ICS networks may create unanticipated "pivot points" and

cascading interdependencies that inadvertently increase the attack surface of both systems;

- Role/responsibility, knowledge/skill/training and other gaps/overlaps between the IT and ICS communities are emerging creating cultural/procedural conflicts

Unlike IT systems, where possible incidents may result in disrupted business operations or loss of information, ICS may face the following incidents:

- Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation;
- Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life;
- Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects;
- ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects;
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment and imperil maintenance staff;
- Interference with the operation of safety systems, which could endanger human life. (*NIST Special Pub 800-82, Revision 2, Draft 2015*)

### ***Differences between IT and ICS Cybersecurity***

Not surprisingly, the differing characteristics and purposes of IT and ICS systems have an impact on their cybersecurity priorities and requirements.

As previously discussed, the three key concepts of information security are Confidentiality, Integrity, and Availability. Availability is considered to be extremely important for ICS while integrity is next in terms of importance and confidentiality is of low importance. In contrast, IT systems prioritize confidentiality and integrity of information stored and transmitted via IT assets and treat system availability as the least important. The following table summarizes the importance placed by IT versus ICS on each information security concept:

**Table 3: IT vs. ICS Security Concept Value**

Priority	IT	SCADA/ICS
#1	Confidentiality	Availability
#2	Integrity	Integrity
#3	Availability	Confidentiality

The major risk impact for IT systems is generally experienced as business operations

delays while the risk impacts for ICS systems are regulatory non-compliance, environmental impacts and loss of life or equipment. For ICS, field devices are a particular cybersecurity concern as many of them are installed in publically accessible locations with little or no physical protection from malicious actions, natural disasters, or from the effects of exposure to the harsh environment of the roadside or roadway.

Another key factor differentiating ICS from enterprise IT systems is ICS' real-time and time-sensitive performance and availability requirements. ICS requirements are more stringent than IT requirements and, for ICS, availability is more important than the data confidentiality as disruptions endanger operations and can affect life safety or environmental quality. ICS must be operational and available 24/7. Therefore, many cybersecurity countermeasures may be infeasible to use with ICS systems. Also, ICS availability requirements may necessitate redundant systems and pre-deployment testing. These requirements also affect the type of access control that may be used. Because ICS systems are time-critical, authorized personnel must be able to access the systems in a timely manner especially during emergencies. On the other hand, IT systems may tolerate some delay and therefore a higher level of access control may be acceptable.

The following table provides a summary of other significant differences.

**Table 4: Differences Between IT vs. ICS (Source: NIST SP-800-82 Rev 2 Draft, 2015)**

Category	Information Technology System	Industrial Control System
<b>Performance Requirements</b>	<p>Non-real-time</p> <p>Response must be consistent</p> <p>High throughput is demanded</p> <p>High delay and jitter may be acceptable</p> <p>Less critical emergency interaction</p> <p>Tightly restricted access control can be implemented to the degree necessary for security</p>	<p>Real-time</p> <p>Response is time-critical</p> <p>Modest throughput is acceptable</p> <p>High delay and/or jitter is not acceptable</p> <p>Response to human and other emergency interaction is critical</p> <p>Access to ICS should be strictly controlled, but should not hamper or interfere with human-machine interaction</p>
<b>Availability (Reliability) Requirements</b>	<p>Responses such as rebooting are acceptable</p> <p>Availability deficiencies can often be tolerated, depending on the system's operational requirements</p>	<p>Responses such as rebooting may not be acceptable because of process availability requirements</p> <p>Availability requirements may necessitate redundant systems</p> <p>Outages must be planned and scheduled days/weeks in advance</p> <p>High availability requires exhaustive pre-deployment testing</p>
<b>Risk Management Requirements</b>	<p>Manage data</p> <p>Data confidentiality and integrity is paramount</p> <p>Fault tolerance is less important – momentary downtime is not a major risk</p> <p>Major risk impact is delay of business operations</p>	<p>Control physical world</p> <p>Human safety is paramount, followed by protection of the process</p> <p>Fault tolerance is essential, even momentary downtime may not be acceptable</p> <p>Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production</p>

<b>System Operation</b>	<p>Systems are designed for use with typical operating systems</p> <p>Upgrades are straightforward with the availability of automated deployment tools</p>	<p>Differing and possibly proprietary operating systems, often without security capabilities built in</p> <p>Software changes must be carefully made, usually by the component manufacturer because of the specialized control algorithms and perhaps the modified hardware and software involved</p>
<b>Resource Constraints</b>	<p>Systems are specified with enough resources to support the addition of third-party applications such as security solutions</p>	<p>Systems are designed to support the intended industrial process and may not have enough memory or computing resources to support the addition of security capabilities</p>
<b>Communications</b>	<p>Standard communications protocols</p> <p>Primarily wired networks with some localized wireless capabilities</p> <p>Typical IT networking practices</p>	<p>Many proprietary and standard communication protocols</p> <p>Several types of communications media used including dedicated wire and wireless (radio and satellite)</p> <p>Networks are complex and sometimes require the expertise of control or signal engineers</p>
<b>Change Management</b>	<p>Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.</p>	<p>Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance. ICS may use OS's that are no longer supported</p>
<b>Managed Support</b>	<p>Allow for diversified support styles</p>	<p>Service support is usually via a single vendor</p>
<b>Component Lifetime</b>	<p>Lifetime on the order of 3-5 years</p>	<p>Lifetime on the order of 10-15 years</p>
<b>Components Location</b>	<p>Components are usually local and easy to access</p>	<p>Components can be isolated, remote, and require extensive physical effort to gain access to them</p>

Similar to the language rift experienced by security and emergency management professionals, terminology shared by one group may not be well-understood or be subtly redefined by the other. Knowledge, skill and experience acquired working in one domain may only be marginally relevant in the other. CIO's of organizations housing both IT and ICS responsibilities need to be sensitive to the very real differences between them and tread cautiously when contemplating fusing their security structures, expecting economies of scale returns.

Unsurprisingly, since the characteristics of ICS and IT are so distinct, so too are their

cybersecurity profiles. The following table outlines key differences between IT and ICS cybersecurity aspects.

**Table 5: : IT vs. ICS Cybersecurity Aspects (Source: APTA Recommended Practice, Part 2)**

Security Topic	Information Technology (IT)	Control Systems (ICS)
Antivirus and Mobile Code	Very common; easily deployed and updated	Can be very difficult due to impact on ICS; legacy systems cannot be fixed
Patch Management	Easily defined; enterprise wide remote and automated	Very long runway to successful patch install; OEM specific; may impact performance
Technology Support Lifetime (Outsourcing)	2-3 years; multiple vendors; ubiquitous upgrades	10-20 years; same vendor
Cybersecurity Testing and Audit (Methods)	Use modern methods	Testing has to be tuned to system; modern methods inappropriate for ICS; fragile equipment breaks
Asset Classification	Common practice and done annually; results drive cybersecurity expenditure	Only performed when obligated; critical asset protection associated with budget costs
Incident Response and Forensics	Easily developed and deployed; some regulatory requirements; embedded in technology	Uncommon beyond system resumption activities; no forensics beyond event re-creation
Physical and Environmental Security	Poor (office systems) to excellent (critical operations systems)	Excellent (operations centers; guards; gates; guns)
Secure Systems Development	Integral part of development process	Usually not part of systems development
Security Compliance	Limited regulatory oversight	Specific regulatory guidance (some sectors)

## ***Highways Operational Systems***

Beginning with the 1986 USDOT Intelligent Vehicle Highway System initiative - later recast in the 1991 ISTEA legislation as Intelligent Transportation Systems (ITS) - the USDOT and its stakeholder partners in government and industry have aggressively pursued the deployment of “electronic and IT applications” to improve transportation safety, enhance mobility and promote environmental sustainability. Throughout the past 25 years, the ITS Joint Program Office responsible for ITS research, standards, and technology transfer has emphasized enterprise data and data interoperability as essential components of the national ITS architectural vision. The National ITS Architecture has included an information security dimension since 2012 (Version 7.0).

Although the national architecture and ITS technical standards make no distinction between deployed IT or ICS systems, applications or technologies, the transportation layer component of the architecture clearly identifies operations subsystems in each of the previously discussed categories (e.g., control systems, SCADA systems, communication systems, toll collection systems and other field deployed systems). This blurring of IT and ICS is also reinforced in the National Architecture’s definitions of the over 100 service packages included in physical subsystem architecture. Some equipment packages, such as *On-Board Emergency Vehicle Barrier System Control* clearly satisfy the definition of ICS-based; others such as the *ITS Data Repository* are just as obviously IT-centric.

The latest version of the ITS strategic plan and the National Architecture also includes priority support for autonomous and connected vehicle subsystems and communications and the deployment of automation of all types, including embedded control and communication automation.

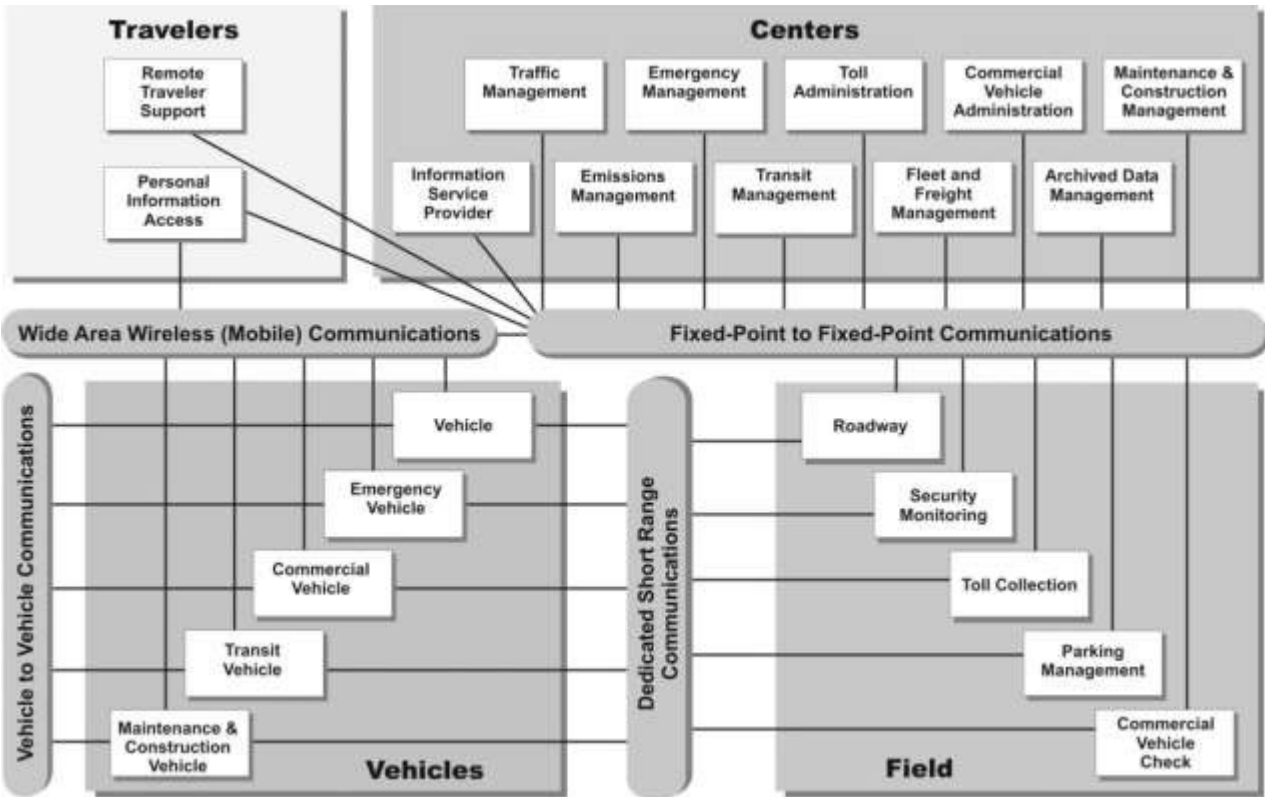


Figure 12: National ITS Architecture 7.1 - Transportation Layer+ . Source: USDOT ITS Joint Program Office

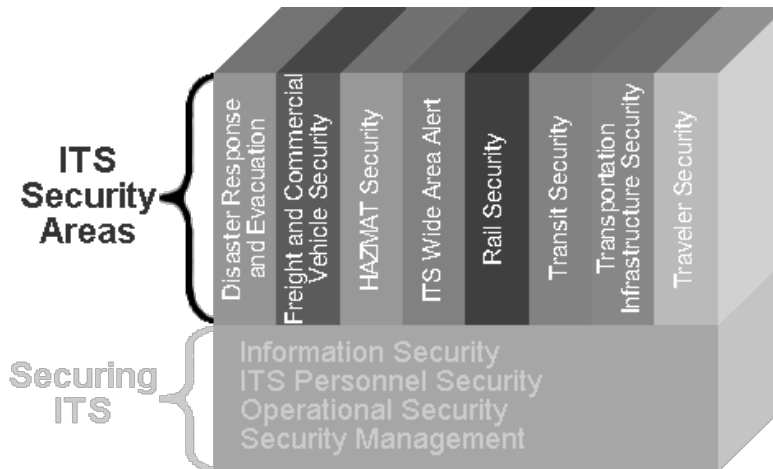


Figure 13: ITS Security Architecture. Source: USDOT ITS Joint Program Office

Moreover, since 2012 the National Architecture has included ITS (i.e., Infrastructure Operations) security areas intended to protect surface transportation infrastructures and also a cross-cutting security function focused on the protection of IT and ICS components of the architecture.

These foundational security services provide security requirements in four inter-related areas:



1. Information (i.e., Data) Security encompassing the origin, transmission and destination of ITS information;
2. Operational (i.e., Physical) Security of information assets focused on the protection of ITS assets from physical and environmental threats;
3. Personnel Security emphasizing the need to protect ITS assets and data from accidental or malicious human activity; and
4. Security Management covering the policy, procedural and administrative dimensions of ITS security while also monitoring and enforcing the processes defined in the Information, Operational and Personnel aspects.

The ITS Security Architecture also identifies potential security services, objectives and threats for each of the Architecture's 15 major information flows and provides security considerations for each of the 22 ITS subsystems and 100 plus service packages.

In part, this was in response to the emerging recognition that the ITS attack surface was much larger than it was at the inception of Program. Four specific dimensions of this issue have been identified as contributing sources of this expanding risk:

1. Use of insecure and aging control devices.
2. Widespread implementation of the National Transportation Communications for ITS Protocol (NTCIP) using open communication channels with increasing reliance on wireless communications. NTCIP is a joint standard that was created by the AASHTO, ITE and NEMA organizations. The NTCIP protocol has very little encryption capabilities because it was assumed that the devices using this protocol would be on a secured network.
3. Integration of multiple agency systems using shared telecommunications networks.
4. Location of much of the distributed ITS field components are in unsecured public areas.

### *Traffic Management Centers*

TMCs use ITS technologies to manage traffic, address incidents, provide travel and incident data and information, and communicate with the region's transportation agencies, media, and other relevant stakeholders. TMCs contain a computer network, application servers, data servers, and wireless peripherals. Field equipment such as sensors transmit information and data back to the TMC for analysis and dissemination. TMCs also control and manage traffic signals to enhance the efficiency of traffic flows. Dynamic message signs help disseminate analyzed information and provide guidance to travelers.

Possible threat agents include terrorists and nation states, organized crime, "hactivists," disgruntled employees, and anyone who desires to tamper with and post messages on dynamic message signs. Common attack surfaces include the following: (Fok, February, 2015)

- Poorly configured field network devices;
- Malware delivered using email or a compromised website;
- Malware walked in by a user either inadvertently or deliberately;
- Compromised partner networks;
- Poorly configured external firewall, switches, or agency webpages;
- Compromised user credentials; and

- Unauthorized physical entry.

In addition, physical design of the TMC and TMC policies (such as allowing public tours) can facilitate breaches. This primer and Ed Fok's 2015 ITE article (cited preciously) provide recommendations on how to counter these cyber threats. These recommendations include use of encryption, an intrusion detection system and "honeypot" to attract/trap attackers, monitoring all data traffic including those from partner agencies and reviewing trusted partner connection policies, and separating the ATIS/511 server from the internal network by moving it to a DMZ.

### ***Transit Operational Systems***

Advanced control and communications technologies have made transit systems safer, more efficient and customer-oriented. For instance, Automated Train Protection constantly monitors the system for potential crashes and prevents them by halting the movement of a train. At the same time, if these technologies are compromised or tampered with, the consequences to life and property may be severe.

These control and communications systems are crucial to the smooth and safe functioning of transit systems. A breach in ICS security can make the transit system vulnerable to severe consequences. Any delay in information flows as well as false information sent to system operators can disrupt normal operations and the functioning of safety systems. Unauthorized changes to commands, ICS software, configuration settings, or alarm thresholds may cause derailments or crashes. (*NIST 2011, APTA Recommended Practice, Part 1 and Part 2*)

According to APTA's Protection Philosophy for rail transit systems, the most critical systems to protect are those that involve the highest risk to life and property: such as the control and communication systems that let the train or train operator start, control the speed of or stop the train. (page 10, *APTA Recommended Practice, Part 2*)

Cybersecurity's role is to ensure that systems including crossings cannot be duped and do not fall under the control of unauthorized persons, and to reduce the chance of human errors. In addition, rail safety systems prevent trains from veering off their prescribed paths or crashing into other trains, vehicles, workers, or pedestrians.

Cybersecurity must protect the safety and reliability of systems to ensure smooth and continued operations. The key aspects of protection include prevention, tamper detection, and auditability. Auditability is the "who, what, where, when, and how" pertaining to cyber incidents. (page 10, *APTA Recommended Practice, Part 2*) Another key protection concept is the separation of zones and avoiding where possible or securing the connection of systems across zones.

Adding to the challenge is the fact that train control and communications systems must often co- exist with legacy systems. Older systems were not intended to be connected to multiple other systems or the internet, and did not anticipate cyber threats. In addition, digital communications have been replacing old, analog communications and offer greater standardization and efficiency. At the same time, additional vulnerabilities have been created. Complicating matters is the longevity of many of the systems.

This section presents certain Transit Operational Systems including Control and Communications Systems. Readers are cautioned that the information provided is of a general nature and may not apply to all installations. Moreover, there are certainly other aspects of these systems important to cybersecurity but not discussed in the Primer.

## Rail Transit Systems

Rail transit systems are complex, cover large distances, integrates many systems, and have control and communications systems located in different areas of the agency: in wayside bungalows, stations, road crossings, signal towers, tunnels, maintenance yards, power stations, refueling depots, equipment storage yards/parking lots, storage depots, local control rooms and operations control rooms. In addition, rail transit systems are publicly accessible and carry large numbers of passengers and accommodate them in stations, and must do so safely.

There are two types of equipment: legacy systems and advanced technology. Legacy systems are standalone systems that are usually isolated from other systems and are not accessible from external sources or devices. These older systems may require different cybersecurity countermeasures than more modern ones and in some cases may not require any additional security. Advanced technology systems, however, are connected to other systems and may be accessible remotely. These systems require cybersecurity measures as well as physical and administrative security. (*APTA Recommended Practice Part I*)

The key components of a rain transit system are:

- Transportation: Rail(s) that guide the train-set including switches to change track/guide and devices built into the track/guide (e.g., to ensure wheel placement).
- Control signaling system: Signals (if present), road crossings and speed controls.
- Communications: Between and among operating trains, crews, station attendants, police and the operations center
- Stations: Below ground, at grade, or above ground. A system may be a mix of these station types.
- Notification methods: Signs, electronic signs, public address (PA) systems, horns and other types of displays
- Train-sets: which may have separate locomotives; these may be powered by different methods.
- Traction power systems: For electrified railways.

More specifically, a transit rail system may include the following systems:

- access control systems
- advertising
- closed-circuit television (CCTV)
- control and communication
- credit card processing
- detection systems for environmental threats (CO, CO<sub>2</sub>, poisons)
- emergency communications

- emergency notification
- emergency ventilation systems
- fare sales/collection
- fire detection/alarms/fire suppression
- grade crossings
- lighting
- passenger information systems
- people-moving systems (elevators, escalators, people movers)
- police dispatch
- pumping systems
- signals and train control
- ticketing systems
- traction power
- vertical lift devices (elevators, escalators)
- vital communication-based train control (CBTC), automatic train protection (ATP) and signaling

### *Train Control and SCADA Systems*

Train control systems provides real-time monitoring of train movements and can also provide automatic train protection or ATP, automatic train operation or ATO, automatic train regulation or ATR, and automatic train supervision or ATS. ATP, a wayside and/or on-board system, automatically applies emergency brakes if a signal is missed. ATO is an on-board system which supports driverless or driver-assist train operations. ATR is an off-board system which works with ATO to support safe and efficient train movements. ATS provides advanced train control, typically including advanced automatic routing and train regulation.

The ***Rail Safety Improvement Act of 2008*** directed the installation of Positive Train Control (PTC) by the end of 2015 although severe resistance from the industry will delay this date for some time. This legislation was introduced in response to a Metrolink train collision on Sept. 12, 2008 where the Metrolink train went through a red signal and crashed into a freight train, killing 25 and injuring 135. PTC is a Communications-Based Train Control (CBTC) technology which automatically protects against train-to-train collisions, excessive train speeds and derailments, and improper movements such as incursions through work zones.

As shown in Figure below, the communications network is the core of the PTC system. PTC systems provide varying degrees of functionality, train control, and automation; and use differing system architectures and wayside systems. If a PTC/CBTC system is compromised, life safety may be affected due to the possibility of derailments and train-to-train collisions.

SCADA systems may or may not be included in train control systems. SCADA systems remotely control and monitor field equipment and systems including control of traction power, control of emergency ventilation systems, and monitoring of drainage pumps and equipment alarms.

Typically, central office (control center) equipment offers supervision, monitoring and dispatch functions; train controllers manage train movement and schedules; and field equipment supplies logic controls. The main components of a rail control center include the following:

- the head-end equipment, including the primary and backup control center;
- the field or slave equipment;
- the transmission media between the head-end and slave equipment ;
- the system networks connecting the head-end components together; and
- the system networks connecting the field components together.

Any necessary connections from train control systems to external devices should incorporate the APTA Recommended Practices. Any internet connections require heightened security measures. Also, field devices can be more vulnerable to attack; once an attacker gains access they may be able to access the central SCADA system due to the trusted nature of the connection.

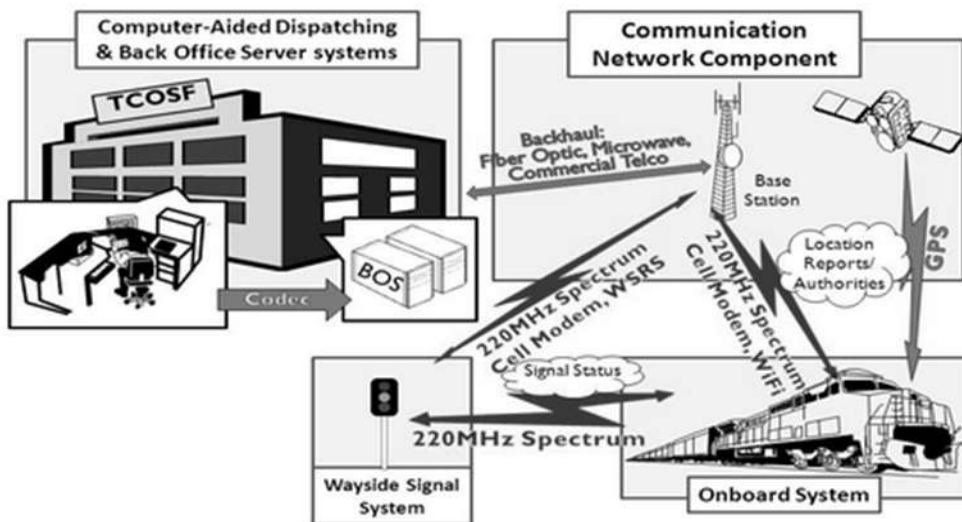


Figure 14: Metrolink's Positive Train Control

Source: <http://www.metrolinktrains.com/agency/page/title/ptc>; Accessed July 2015

Cyber threats and threat vectors apply to Train Control and SCADA systems. Even though some cyber threats do not intend to harm passengers or transit infrastructure, their tools may still infect train control and SCADA systems and inflict considerable physical as well as system damage. Furthermore, vulnerabilities in these systems can facilitate threat vectors in carrying out their missions.

### *Communication Systems*

Examples of communications systems include CCTV, radio, intercom, public address, security, and copper and fiber optic data transmission systems. They may or may not be connected to other systems.

Surface radio systems allow surface communications with maintenance and other non-revenue vehicles. Surface vehicle radio systems allow communications between vehicle operators and the control center. Subway radios allow communications with vehicles and personnel below ground. Emergency services radio systems can reach below-ground areas through retransmission through transit agency equipment or another system.

Phone service includes emergency, maintenance and administrative phones, and passenger assistance intercoms at stations, waysides, and yards.

Electronic passenger information displays at station platforms transmit messages from the control center to passengers. Public address systems can also provide real-time train and system information.

### *Security Control and Detection Systems*

Transit facilities require monitoring to restrict physical access to the system. Technologies used for intrusion/access control include CCTV's, perimeter detection, and card access. Closed-circuit television (CCTV) systems are used for surveillance, deterrence and detection purposes. They may be connected with physical intrusion detection and intercom systems and may allow recordings. Since CCTV systems are now digital and enable wireless uploads to computers and servers, cybersecurity needs to be incorporated into the system design. For additional information, see *APTA Recommended Practice Selecting Cameras, Recording Systems, High-Speed Networks and Trainlines for CCTV Systems*.

Other threat monitoring/detection systems that alarm when a specific threat/condition is detected include Fire Detection, Elevating Devices Monitoring, Tunnel Drainage Monitoring, Gas and Pathogen Monitoring, and Seismic Monitoring. Underground stations have emergency management panels which integrate alarms, phone, PA, elevator/escalator, ventilation and other controls and systems.

### *Data Transmission*

Data transmission may occur through physical or wireless methods. Physical methods include fiber optic network, copper network, and leased lines. Fiber optic network has higher bandwidth than copper network and is used for transmission between the control center and passenger stations, electrical substations, and other transit facilities. Copper networks are used for short-run Local Area Network (LAN) transmissions. Leased lines are used for Wide Area Network (WAN) data and voice transmissions.

Wireless communication-based systems include Communications-Based Train Control, positive train control, SCADA and local monitoring and control. Wireless may not be appropriate for time-critical applications. In any case, the use of multiple technologies versus a single technology is advisable.

### *Fare Collection Systems*

Fare collection systems are used not only for revenue collection purposes but for ridership counts as well. These systems can include the following equipment and technologies: fare boxes, automated passenger counters, fare validators, entry/exit gates, handicapped-accessible gates, emergency gates, GPS, radio systems, ticket vending machines, ticket office machines, and parking machines.

Theft of service and selling spoofed fare media are often the intent of hackers. Also, vending

machines accept credit cards and debit cards making them attractive targets of criminals. Recently, skimming devices were discovered in the MTA LIRR and NYCT vending machines.

#### *Vehicle Monitoring Systems for Surface Systems*

Vehicle monitoring systems include automatic vehicle monitoring (AVM) for surface systems such as buses and streetcars. Note that vehicle monitoring systems for rail transit are included in train control systems.

#### *Automatic Vehicle Location (AVL) System*

AVL systems are used in fixed route and demand response transit systems in conjunction with Computer-Aided Dispatch (CAD) systems to locate and more efficiently manage transit bus and demand response vehicle fleets. The primary elements of the AVL system include an on-board computer, GPS, and mobile data communications.

#### *Train Control Systems (TCS)*

Train control systems were described earlier.

#### *Traction Power Control*

The SCADA system provides traction power control which monitors and controls electrical substation equipment at electrical substations and along the rapid transit ROW. Newer systems are PLC-based.

#### *Ventilation Control*

The SCADA system also provides ventilation control which monitors and operates fans, dampers, and doors. These systems can be controlled from a central control center or from individual stations. Newer systems are PLC-based.

#### *Fully Integrated Systems*

A fully integrated system will perform the remote monitoring, control, and data collection functions using a common client/server architecture which is connected to various devices including field equipment. While these systems have benefits, security issues can arise with

these systems as they are interconnected and serve many users.

### *System Boundaries and Interfaces*

All system boundaries and interfaces to other systems should be identified, catalogued, and secured. These include local ports for direct connection, internet connections, intranet and extranet connections, and modem-based connections.

## **Surface Transportation Cybersecurity Issues**

In spite of staggering amounts of time, money and effort being spent on cybersecurity initiatives across the industry, some issues are considered to be intractable and persistent.

- Resilience – In this context, resilience refers to the ability of a system to operate adequately when stressed by unexpected or invalid inputs, subsystem failures or extreme environmental conditions.
- Privacy - The ability of a system to protect sensitive information from unauthorized access by humans or machines.
- Malicious Attacks – the ability to deter and recover from internal vulnerability exploits even in “air-gapped” systems.
- Intrusion Detection – The ability of a system to monitor its internal baseline “normal” operating parameters and issue an alert when deviations are detected.

Indeed, as increasingly complex combinations of computation, networking and process, interconnected with an array of feedback loops, connecting humans and machines begin to resemble “living” organisms and ecosystems, new models of cybersecurity are beginning to emerge. Concepts borrowed from human physiology such as active and passive immune functions are being researched with the intent to replace already impotent strategies such as “defense-in-depth.” The addition of tens of millions of connected vehicles and their “smart slab” enabled owners will only accelerate the need for more subtle solutions.

## **Emerging Trends in Transportation Control Technologies**

1. Connected Vehicle program
2. Machine to Machine (M2M)
3. Transportation Management Centers (TMCs)
4. Big Data and Preventive Maintenance
5. “Bring your Own Device” (BYOD)

### *Connected Vehicle Program*

USDOT’s Connected Vehicle research program addresses key transportation challenges – vehicle crashes, congestion, and pollution through the following technology areas.

#### Safety

- Vehicle-to-Vehicle (V2V)
- Vehicle-to-Infrastructure

#### (V2I) Mobility



- Dynamic Mobility Applications Environment
- AERIS
- Road Weather Applications

Fifty billion connected vehicles are anticipated to be on the road within a decade. Accompanying these vehicles will be Machine to Machine (M2M) devices sending and receiving data through wireless solutions.

Auto makers, fleet managers, and DOTs are working towards the centralized control of systems with the connected vehicles; however, the many peripheral, aftermarket devices and software not within this centralized control has introduced potential vulnerabilities as they access various elements of the connected vehicles.

A 2015 Wired magazine article, *Hackers Remotely Kill Jeep on Highway*, described a demonstration, with the driver's consent, of taking remote control of a Jeep Cherokee, causing unexpected dashboard activity and the vehicle to slow to a crawl on a busy interstate highway. While this incident was planned, it serves to illustrate the vulnerability of vehicles to cyber attacks.

*I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold. Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass. (<http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> accessed July 28, 2015)*

Security and privacy are key policy issues being considered and addressed in the program. Security challenges include message validity, security entity, network security, security operations business models, and equipment and system certification processes. Privacy issues include the ability of users to opt out of tracking applications and activities.

A common framework for Connected Vehicle technologies and interfaces is under development and will include Enterprise, Functional, Physical, and Communications views. Various applications have been developed or are under development. Pilot tests have also been completed or are underway. (*Robert Sheehan, Connected Vehicle Research Program Presentation, ITSJPO, USDOT*)

**Safety.** The Connected Vehicle's safety program is expected to prevent or mitigate as much as 80% of crashes caused by unimpaired drivers through the implementation of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) safety applications. V2V applications include Forward Collision Warning, Blind Spot/Lane Change Warning, Do Not Pass Warning, Left Turn Assist, and Intersection Movement Assist. V2I applications include Curve Speed Warning, Red Light Violation Warning, Stop Sign Gap Assist, and Transit Pedestrian

Warning. (*Robert Sheehan, Connected Vehicle Research Program Presentation, ITSJPO, USDOT*)

At the same time, this program may exponentially increase the number of vehicles accessible by hackers and bad actors through the implementation of Dedicated Short Range Communications (DSRC) between vehicles, between vehicles and the roadway, between vehicles and traffic signals and other infrastructure, and between vehicles and pedestrians and obstacles.

A key security feature which will be included in the program is the Security Credential Management System (SCMS) currently under development. The system will ensure the integrity of V2V and V2I applications and anonymity of data emanating from vehicles and traffic signals. As shown in the accompanying figure, the SCMS will be focused on security and privacy by design and will include on-board security elements and security of interactions between on-board elements and the SCMS. (*RITA/USDOT, Security Credential Management System Design, April, 2013; Drew Van Duren, FHWA Presentation Slides on Cybersecurity TRB: Connected Vehicles Security, Oct., 2014*)

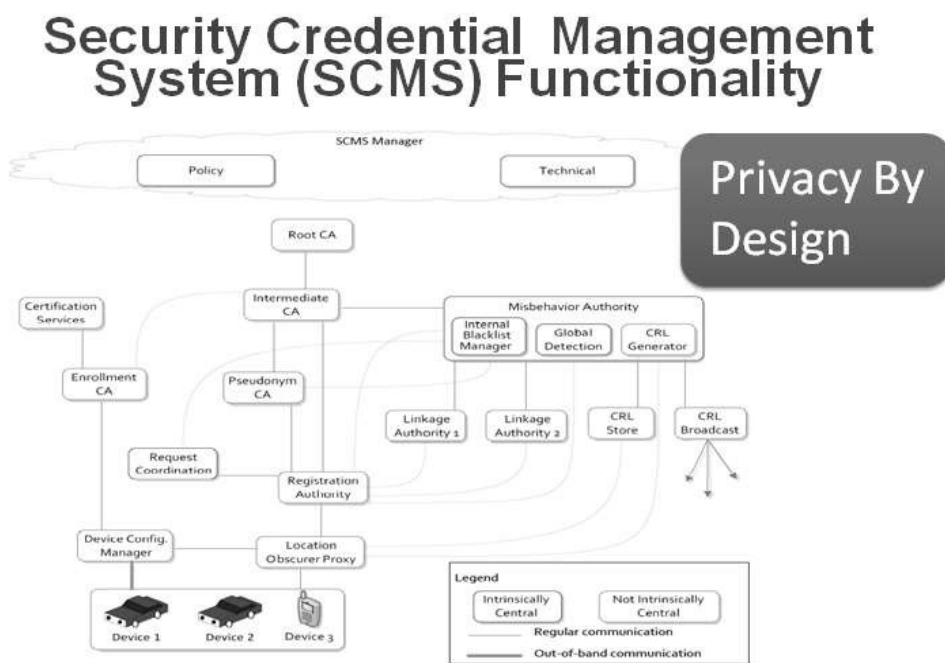


Figure 15: : Security Credential Management System (SCMS) Functionality

Source: Van Duren, FHWA, Presentation Slides on Cybersecurity TRB: Connected Vehicles Security, Oct., 2014

**Mobility.** The Mobility program includes applications such as the Multimodal Intelligent Traffic Signal System; Intelligent Network Flow Optimization; Response, Emergency Staging and Communications, Uniform Management, and Evacuation; and the Enable Advanced Traveler Information Systems.

Road user mobility concerns include integrity, availability, and privacy/anonymity of data including payment data. These concerns will likely increase as more and more road users utilize mobility services and applications. Appropriate policies and user authentication methods

can mitigate these issues. The public transportation, freight carriers, taxis, and emergency responders use fleet management systems, automated vehicle location (AVL) and computer-aided dispatch (CAD) technologies to track and manage buses, trucks, and other fleets.

**Environment.** The Environment program contains AERIS applications such as Eco-Integrated Corridor Management and Eco-Traveler Information and road weather applications. While these may be less attractive targets to potential hackers, any vulnerability in these applications may potentially lead to the compromising of safety critical systems.

**Machine to Machine M2M (Internet of Things).** White-hat security tests of intelligent vehicles and their electronic components have proven that they are indeed vulnerable to hackers; however, as the required effort was high only sophisticated hackers will be able to launch successful attacks. (*ITSA Connected Vehicle Assessment Report (2012-2014)*) At the same time, aftermarket mobile applications are proliferating, making mobile security an increased concern for transportation providers. Examples of these applications include location-based mapping and navigation software and real-time traffic incident alerting applications for drivers, and real-time next-bus arrival information and transit delay alerting applications for transit customers. These applications may have lax security measures especially when storing user location and other user-associated data. The ITSA report notes that while documented vulnerabilities have increased and mobile devices are subject to theft, operating systems for mobile devices are more secure than those using legacy systems.

M2M is used to deliver these technology applications and offer numerous benefits to drivers such as automated diagnostics of safety systems and driver alerts regarding necessary engine maintenance. When the manufacturer offers M2M, testing for safety and cybersecurity issues is typically performed. However, aftermarket devices and applications used by the traveling public provide them with significant benefits and convenience but use open platforms and have specific security vulnerabilities as well. As noted in the *ITSA Connected Vehicle Assessment report (2012-2014)*, most vulnerabilities arise from design flaws and bugs in software and the best long-term countermeasure is quality software and the actions (requirements definitions, reduction in system complexity) that lead to such software. Also, they use wireless communications that may be attacked from a long distance from the network. In addition, bugs in wireless systems cannot easily be eliminated. Additional issues include authentication, telecommunications carrier “insider” threats, and denial of service. Connections with ATIS/511 traveler information servers can provide a way for hackers to penetrate the TMC’s network.

### *Connected Vehicles Technology System Types*

The three technology system types for connected vehicles include:

- Operation Technology (OT)
- Information Technology (IT)
- Networking and Communications

Operational Technology (OT) is product- or system-oriented and includes automotive electronics and traffic management systems. OT systems are usually safety and operational

critical systems and therefore availability and integrity are paramount. While legacy OT was isolated, next generation OT is not. Next generation OT makes use of “Internet of Things” applications. “Internet of Things” link objects and formerly unconnected systems to the internet using standardized protocols and architectures; this standardization, in turn, makes it easier for hackers to access the next generation OT systems. (*ITSA Connected Vehicle Assessment – Cybersecurity and Dependable Transportation, Connected Vehicle Technology Scan Series, 2012-2014*)

## IT

IT risk stems primarily from third-party software used by the traveling public. In addition, sub-optimal software design, security measures and patch management are also key cybersecurity issues for IT. IT attack vector categories include unauthorized access, malicious code, and reconnaissance and networking-based service attacks.

### *Networking and Communications Systems*

Networking and communications vulnerabilities include security protocols, authentication of communication partners, telecommunications threats, and denial of service.

Wireless networks used for transmission of connected vehicle and traffic data are vulnerable to attack from miles away. Also, telecommunications infrastructure vulnerabilities are difficult to address and have tended to remain unaddressed for years after they are discovered. Telecommunications insiders also pose a threat as they have access to subscriber information. The *2014 NHTSA Cybersecurity Best Practices* report makes the observation that the telecommunications industry supply the wireless services used for ITS and other automotive services, and that the telecommunications industry along with the internet have, at the same time, facilitated hackers as well.

The USDOT in conjunction with the public and private sectors is developing DSRC communications standards, interface standards for other media, and information exchange standards.

NHTSA sponsored research into cybersecurity best practices applicable to automotive cybersecurity by reviewing and analyzing industry practices of IT and telecommunications, NIST, industrial control and energy, aviation, financial payments, and medical devices. The report also presents an Information Security Lifecycle consisting of the Assessment, Design, Operation, and Implementation Phases. The research was conducted by the VOLPE Center.

### *Big Data and Preventive Maintenance*

Big Data and Preventive Maintenance: ITS produces large amounts of data or “Big Data” – there are many positive uses for this data including the creation of predictive algorithms to determine future congestion and traffic patterns, and likely incident locations. There are also predictive maintenance applications based on data which will be generated through the Connected Vehicle program. Weaknesses in data storage policies and practices can expose

individual financial data and location-based data to hackers. Also, compromised data can result in no or incorrect maintenance alerts being issued to drivers and vehicle owners.

### *Bring Your Own Devices (BYOD)*

The Bring Your Own Devices practice of TMC employees and contractors can introduce vulnerabilities into the TMC environment. BYOD use wireless networks that are prone to hacking. Hence, BYOD policies and procedures should be established and enforced.

### ***Transportation Roadmap for Cybersecurity***

In August of 2012, the U.S. Department of Homeland Security's (DHS's) National Cybersecurity Division (NCSD), Control Systems Security Program (CSSP) released ***The Roadmap to Secure Control Systems in the Transportation Sector*** (Transportation Roadmap, a voluntary framework for improving the cybersecurity across all transportation modes). The Transportation Roadmap is intended to act as a template for action for individual organizations and provides a series of activities and benchmarks used *“to identify the cybersecurity features currently in place and to determine the next activities for consideration to improve cybersecurity performance.”*

The Roadmap proposes four national cybersecurity goals with corresponding end states and consistent with the National Policy Guidance extant in 2012. Each goal is supported by multiple objectives, milestones and metrics to be accomplished over three timeframes encompassing a 10- year planning horizon. As new or modified Policy Guidance becomes available, and as significant accomplishments occur, DHS, DOT and other key stakeholders will need to revisit and revise the Roadmap.

Two years after the release of the US Transportation Roadmap, the SECUR-ED Urban Transportation – European Demonstration (SECUR-ED) released an international version of the ***Cybersecurity Roadmap for Public Transportation Operators (PTO's)***. Although the primary audience for this document was European transit agencies, the document provides much information of use to US operators. Topics included address:

- How cybersecurity fits in the overall risk management strategy of a PTO;
- A comprehensive framework of assets, architectures and technologies used by a PTO taking into account the different types of transport operated by PTO's as well as the cases where the transport operator is not the infrastructure owner;
- A set of security standards and regulations that may be applicable to a PTO;
- How cybersecurity will impact PTO organizations;
- A set of baseline security requirements for future procurement;
- An implementation approach and first affordable security measures;
- Further directions towards standardization and eventually regulation.

## Chapter 5 Countermeasures: Protection of Operational Systems

There are countermeasures and approaches that transportation agencies can utilize to reduce risks and mitigate impacts of cyber incidents. Significant work has been accomplished in cybersecurity, especially in the areas of IT/network security and most recently in control system (ICS) cybersecurity. The National Institute of Standards and Technology (NIST), the Federal Information Processing Standards (FIPS), with transportation specific guidance available from APTA and FHWA, have developed recommended practices and standards. There are international standards and recommendations from the International Organization for Standardization (ISO), the Information Systems Audit and the Control Association (ISACA), and Control Objectives for Information and related Technology (COBIT).

Security working groups such as the Computer Security Incident Response Team (CSIRT) and the Computer Emergency Response Team (CERT), and ICS CERT, which responds to breaches of cybersecurity, have compiled resources of recommended practices that can be applied across all industries. This section provides high-level approaches to reduce vulnerabilities and mitigate impacts of incidents and an overview by category, of specific areas to address as part of cybersecurity.

### Selected Technical Guidance

*NIST SP 800-62 Guide to Industrial Control Systems (ICS) Security, 2nd Edition, 2015.*

*NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations, 2009.*

*APTA Recommended Practice: Securing Control and Communications Systems in Rail Transit Environments Parts I, II and III*

*Critical Controls for Effective Cyber Defense, 20 Critical Security Controls - Version 4.1, COBIT, 2013*

*21 Steps to Improve Cyber Security of SCADA Networks, U.S. Department of Energy, Infrastructure Security and Energy Restoration Committee, 2007*

There are some countermeasure resources that provide comprehensive guidance and recommendations for a broad range of risks. For example ***The Critical Controls for Effective Cyber Defense (COBIT, 2013)*** is consensus list of the best techniques that

*“reflect the combined knowledge of actual attacks and effective defenses of experts in the many organizations that have exclusive and deep knowledge about current threats. These experts come from multiple agencies of the U.S. Department of Defense, Nuclear Laboratories of the U.S. Department of Energy, the U.S. Computer Emergency Readiness Team of the U.S. Department of Homeland Security, the United Kingdom's Centre for the Protection of Critical Infrastructure, the FBI and other law enforcement agencies, the Australian Defence Signals Directorate and government and civilian penetration testers and incident handlers.”*

The chart on the following page summarizes of the critical controls best practices, ranked by effectiveness in mitigating incidents. The controls are broken into four groups: (1) those that

address operational conditions that are “actively targeted and exploited”, (2) those that address known “initial entry points”, (3) those that “reduce the attack surface, address known propagation techniques” and mitigate the impact of an incident, and (4) those related to “optimizing, validating and managing”.

Critical Control	Effect on Attack Mitigation	
Critical Control 1: Inventory of Authorized and Unauthorized Devices	Very High	These controls address operational conditions that are actively targeted and exploited by all threats
Critical Control 2: Inventory of Authorized and Unauthorized Software	Very High	
Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers	Very High	
Critical Control 4: Continuous Vulnerability Assessment and Remediation	Very High	These controls address known initial entry points for targeted attacks
Critical Control 5: Malware Defences	High	
Critical Control 6: Application Software Security	High	
Critical Control 7: Wireless Device Control	High	These controls reduce the attack surface, address known propagation techniques, and/or mitigate impact
Critical Control 8: Data Recovery Capability	Moderately High to High	
Critical Control 9: Security Skills Assessment and Appropriate Training to Fill Gaps	Moderately High	
Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	Moderately to Moderate High	These controls are about optimizing, validating and/or effectively managing controls.
Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	Moderate	
Critical Control 12: Controlled Use of Administrative Privileges	Moderate	
Critical Control 13: Boundary Defence	Moderate	
Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	Moderate	
Critical Control 15: Controlled Access Based on the Need to Know	Moderately Low to Moderate	
Critical Control 16: Account Monitoring and Control	Moderately Low to Moderate	
Critical Control 17: Data Loss Prevention	Low	
Critical Control 18: Incident Response Capability	Low	

Figure 16: : Summary of Critical Controls Best Practices. Source: COBIT

As part of the Critical Controls, five "quick wins" or the "First Five" were identified. These controls have been found to be “the most effective means yet found to stop the wave of targeted intrusions that are doing the greatest damage to many organizations.” The "First Five" address:

1. Software white listing
2. Secure standard configurations
3. Application security patch installation
4. System security patch installation
5. Ensuring administrative privileges are not active while browsing the web or handling email.

Recommended practices for cybersecurity typically are grouped into categories. For example, the *NIST Cybersecurity Framework* includes the following under Protection:

- Access Control
- Awareness and Training
- Data Security and Information Protection
- Protective Technology

Other categorizations also highlight

- Cyber Hygiene
- Boundary Defense and Network Separation
- Configuration Management

The rest of this chapter will address each of these in turn, starting with cyber hygiene – the basic practices that can improve cybersecurity.

## Cyber Hygiene

Annual cybersecurity surveys regularly find that only a small percentage of cyber breaches (3% in 2012) were unavoidable without difficult or expensive actions.

- Most successful breaches (more than 90% in 2012) required only the most basic techniques to be eliminated.
- Almost all (97% in 2012) of successful breaches could have been avoided if simple or intermediate controls were in place
- 75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching.

(Source: *Symantec Internet Security Threat Report Trends and Verizon Data Breach Investigations Report*)

### Basic Rules of Cyber Hygiene

- Update systems and software, including keeping patch levels up to date.
- Maintain up-to-date antivirus, if available, and apply based on control system vendor recommendations.
- Use strong passwords and change default passwords often.
- Remove or disable any unused applications or functions. Build systems with only essential applications and components required to perform the intended function.
- Limit use of removable storage devices (USB thumb drives, external drives, CDs).
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.

### Control System Considerations

- IT patching typically requires relatively frequent downtime. Any sudden or unexpected downtime of control systems can have serious operational consequences.
- Control systems may not be able to run anti-virus software.
- Control system devices may be hard-coded or "insecure by design".
- Control system devices may be exposed to Internet without agency awareness.

Common cyber hygiene practices include:

1. Encouraging staff to follow basic security policies and procedures.
  - Not giving out user names, passwords, or other access codes to anyone.
  - Not opening e-mails or attachments from strangers.
  - Not installing or connecting any personal software or hardware to organization's



network or hardware without permission.

- Making passwords complex and changing passwords regularly (every 45-90 days).
  - Keeping anti-virus software current. Regularly downloading and installing vendor security "patches".
  - Following Bring Your Own Device (BYOD) and mobile device management (MDM) security practices.
2. Removing unnecessary applications and functions from systems.
    - Reducing or removing general purpose services/interfaces.
    - Using application specific-least functionality interfaces.
    - Reducing static open file exchanges (shared folders).
    - Eliminating hidden hubs.
  3. Changing default configuration options and passwords such as manufacturer or vendor's default passwords.

#### **Basics Count Case Study: 75 Airports Impacted**

In the summer 2013, the Center for Internet Security (CIS) was notified of a potential Advanced Persistent Threat (APT) incident at four airports in the U.S. An investigation found it eventually impacted 75 airports with 2 airports confirmed to have been compromised. As summarized in the ICS-CERT Alert on this incident (ICS-ALERT-14-176-02A), the APT campaign used phishing emails, redirects to compromised web sites and most recently, trojanized update installers on at least 3 vendor web sites, something known as watering hole-style attacks. CIS identified a public document related to the aviation industry that appeared to be the source used by the attackers to select the phishing email victims. This incident is a very real reminder that basic cybersecurity does matter.

#### **Selected Cyber Hygiene Technical Resources: *NIST SP 800-118, Guide to Enterprise Password Management***

*NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook.*

*NIST SP 800-40, Creating a Patch and Vulnerability Management Program, 2005.*

*Mix, S., Supervisory Control and Data Acquisition (SCADA) Systems Security Guide, EPRI, 2003.*

*Dzung, D., Naedele, M., Von Hoff, T., and Crevatin,*

*M. "Security for Industrial Communication Systems," Proceedings of the IEEE. Institute of Electrical and Electronics Engineers Inc. 2005.*

*NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, 2015.*

*NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.*

#### **Access Control**

Access control involves maintaining secure access to assets and associated facilities, limiting it to authorized users, processes, or devices, and to

authorized activities and transactions. Cybersecurity access control cannot be easily separated from physical security. Inadequate physical security can put cyber assets in

jeopardy. Physical damage can compromise cyber assets. This section only addresses the cyber components of access control. See *NCHRP Report 525 Surface Transportation Security, Volume 14 Security 101: A Physical Security Primer for Transportation Agencies* for additional information and resources.

#### **Access Control Basics**

- Use strong passwords and change default passwords often.
- Restrict physical access to the network and remote devices.
- Disable unused ports and services on ICS devices after testing to assure this will not impact ICS operation.
- Restrict user privileges to only those that are required to perform each person's job (i.e., establish role-based access control and configure role based on principle of least privilege).
- Consider the use of two-factor authentication methods for accessing privileged accounts or systems.
- Consider using separate authentication mechanisms and credentials for users of the TMS system network and corporate network.
- When remote access is required, consider deploying two-factor authentication through a hardened IPsec/VPN gateway with split-tunneling prohibited for secure remote access. Be prepared to operate without remote access if required.

#### **Control System Considerations**

- Apply appropriate access controls to all field devices such as ramp/gate/signal controllers, dynamic messaging signs, switches, and signaling devices.
- Secure remote access channels, e.g. place remote devices on private networks if possible.
- Disable telnet, webpage, and web LCD interfaces if not needed.

Effective access control includes applying the concept of least-privilege. Every program and every user of the system should operate using the least set of privileges necessary to complete the job. It is also recommended to place controls between network segments, if possible, to limit congestion and cascading effects which will mitigate the effects of an incident that does occur.

In addition, it is important to identifying controls to minimize the consequences from human error and other unintentional incidents such as equipment failure.

### **Access Control Case Study: Dynamic Messaging Signs**

In recent years, dynamic message signs have been a frequent target for mischief. With instructions online and default passwords never reset, anyone could, and did, change the signs to show humorous or profane messages. In 2014, a hacker calling himself Sun Hacker, remotely accessed a DOT network and changed multiple signs at once. This demonstrated to the FWHA and ICS-CERT the ability to do more serious damage. As summarized in the ICS-CERT Alert on this incident (ICS –ALERT-14-155-01A), there was initial concern that the units involved had hard-coded passwords but the vendor confirmed that changes could be made during unit installation.

### **Selected Access Control Technical Resources:**

*NIST SP: 800-73-2, Interfaces for Personal Identity Verification (4 parts), September 2008.*

*NIST SP 800-76-1, Biometric Data Specification for Personal Identity Verification, 2007.*

*NIST SP: 800-57 Recommendation for Key Management, March 2007*

*Part 1, General (Revised) Part 2, Best Practices*

*Part 3, Application Specific Key Management Guidance (Draft), October 2008*

*NIST SP 800-82 Rev 1, Guide to Industrial Control Systems (ICS) Security, May 13, 2013.*

*Mix, S., Supervisory Control and Data Acquisition (SCADA) Systems Security Guide, EPRI, 2003.*

*Baker, Elaine, et al, NIST SP: 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007.*

*NIST SP: 800-118, Guide to Enterprise Password Management*

*NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.*

*Dzung, D., Naedele, M., Von Hoff, T., and Crevatin, M. "Security for Industrial Communication Systems," Proceedings of the IEEE. Institute of Electrical and Electronics Engineers Inc. 2005.*

*NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, 2015.*

*NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, 2013.*

### **Data Security and Information Protection**

Transportation agencies have a broad range of data collected and stored on their networks. Along with traffic control and system data, there is personally identifiable information (PII) of employees, contractors and often, customers. Agencies may have credit card information and a few, those which have responsibility for the state Department of Motor Vehicles (DMV) have extensive customer personal information. Data security means that information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality (preserving authorized restrictions on information access and disclosure), integrity (guarding against improper information modification or destruction), and availability (ensuring timely and reliable access to and use of information) of information.

NIST SP800-53 Recommended Security Controls for Federal Information Systems and

Organizations includes an extensive catalog of management, operational and technical security controls that can be applied to transportation agencies as well.

### **Data Security and Information Protection Basics**

- Protect data-at-rest and data-in-transit with encryption, when possible. Move data between networks using secure, authenticated, and encrypted mechanisms. Perform an annual review of algorithms and key lengths in use for protection of sensitive data.
- Implement protections against data leaks and loss. Data Loss Protection controls are policy based and include classifying sensitive data, identifying sensitive data across the agency, enforcing data security controls, and on-going reporting and auditing to ensure policy compliance.
- Ensure that data assets are formally managed throughout removal, transfers, and disposition. Backups of data and information are conducted, maintained, and tested periodically. Data is destroyed according to security policy.
- Adequate data capacity is maintained to ensure availability.
- Review cloud provider security practices for data protection.
- Integrity checking mechanisms are used to verify software, firmware, and information integrity.
- The development and testing environment(s) are separate from the production environment.

### **Control System Considerations**

- Communications protocols used in control systems environments are different from IT protocols.
- Available computing resources (including CPU time and memory) are limited, so may not have enough memory and computing resources to support addition of security capabilities.
- Some of the operating systems and applications running on ICS may not operate correctly with commercial off-the-shelf IT cybersecurity solutions. In some instances, vendor license and service agreements may not allow third-party cybersecurity solutions.
- Encryption capabilities, error logging and password protection may not be available.

**Data Security Case Study:  
Customer Information Leaked**

In 2011, Internet activist group Anonymous defaced a transit agency's customer facing website and released the personal contact information of agency users. As part of a political protest, Anonymous posted what it said was the User Database and included names, addresses, phone numbers and email accounts. In a group statement about the posting, Anonymous told customers to contact the transit agency and "ask them why your information wasn't secure with them."

**Selected Data Security Technical Resources:  
*NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, 2013.***

*NIST SP: 800-57 Recommendation for Key Management, March 2007*

*Part 1, General (Revised)*

*Part 2, Best Practices*

*Part 3, Application Specific Key Management Guidance (Draft), October 2008*

*NIST SP 800-82 Rev 1, Guide to Industrial Control Systems (ICS) Security, May 13, 2013.*

*NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.*

***Boundary Defense and Network Separation***

Protecting the boundaries of systems and separating networks are critical to cybersecurity. The edges of systems – for many reasons – are the most vulnerable spots. Implementing technical defenses such as firewalls are a common recommended practice. A strong system of network firewalls includes an external firewall to protect from unauthorized persons trying to get into the network and internal firewalls to wall off different departments/divisions. Those areas that contain the most critical applications and sensitive or valuable information should have particularly robust protections from each other.

As many sources have noted, firewalls are not complete solutions. There are coverage and accuracy issues that have to be considered, along with the likelihood that individual components have direct or wireless connections to the Internet through unknown or unapproved channels. For example, printers on the network may have wireless connections.

For SCADA and control system networks, the connections between remote field devices, e.g. remote access units (RTU) or programmable logic controllers (PLC), to the master terminal unit (MTU) are of primary concern. Firewalls between MTUs and RTUs are critical in any system architecture. However, because commercial firewalls do not generally support SCADA protocols, SCADA protocols and the types of ports using the protocols have to be identified and opened in the firewalls for the system. Unfortunately, security experts have long known that one of the great vulnerabilities in a network is the inadvertent opening of ports that can be attacked.

Providing adequate network segmentation between control and business networks is another

recommended practice. In some transportation systems, physical isolation of one network from another or air gapping, has been considered as a security technique. In the past, transportation systems may have been closed proprietary systems protected by “air gaps” and “security by obscurity”, but over time isolated systems shifted to more connected systems including connectivity to safety-critical control systems found in vehicles and in Advanced Traffic Management Systems. In addition, due to the human factor there is no true air gap. Users can, and often do create, a connection through external devices (using USB sticks, thumb drives, laptop connections, VPN, DVDs, etc.)

#### **Boundary Protection and Network Separation Basics**

- Provide logical separation between the corporate and control system networks (e.g., stateful inspection firewall(s) between the networks, unidirectional gateways).
- Employ a DMZ network architecture (i.e., prevent direct traffic between the corporate and control system networks).
- Disable unused ports and services on control system devices after testing to assure this will not impact operation.
- When remote access is required, consider deploying two-factor authentication through a hardened IPsec/VPN gateway with split-tunneling prohibited for secure remote access. Be prepared to operate without remote access if required.

#### **Control System Considerations**

- Commercial firewalls do not generally support SCADA/control system protocols.
- Secure connections between remote field devices, e.g. remote access units (RTU) or programmable logic controllers (PLC), to the master terminal unit (MTU).

The following figures provide a typical highway transportation system network and recommendations.

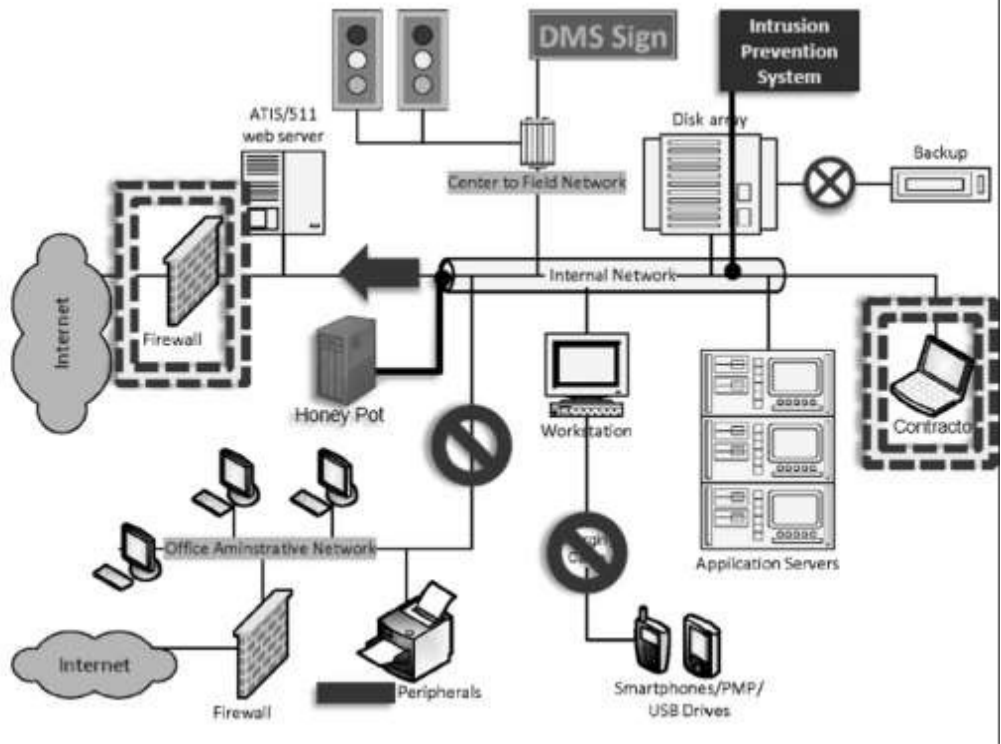


Figure 17: Typical Transportation System Network with Countermeasures

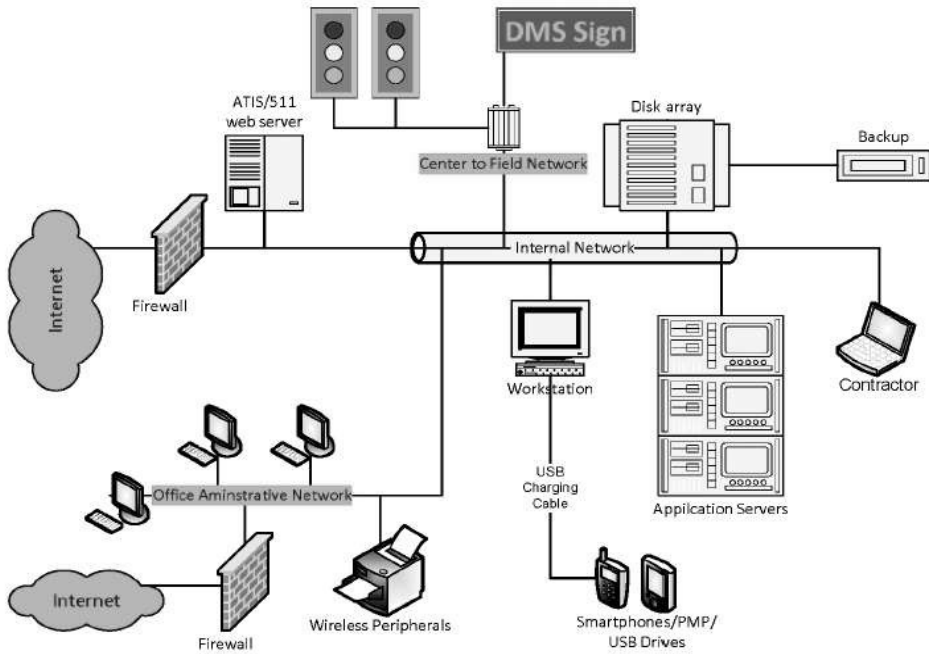


Figure 18: Typical Transportation System Network without Countermeasures

It is critical to be aware of how and what systems are connected in agency networks. For example, it is not uncommon to connect HVAC equipment to the rest of the network. The access for the 2013 Target credit card breach was through the HVAC system. After the Target incident, an estimate was made of vulnerable HVAC systems and over 55000 internet connected systems were found. Most may not even be aware the HVAC system can be found through the web and may not be paying attention to the connections it has to other systems on the network.

### **Network Separation Case Study:**

#### **HVAC Systems**

It is not uncommon for HVAC equipment to be connected to enterprise networks. An FBI Cyber Alert noted that 55,000+ HVACs had known vulnerabilities. Best practice for any system would be to have it on a separate network, if possible, and to understand any remote access used by the vendor for maintenance and monitoring of the HVAC system.

### **Selected Boundary Protection and Network Separation Technical Resources:**

*NIST SP: 800-73-2, Interfaces for Personal Identity Verification (4 parts), September 2008.*

*NIST SP 800-76-1, Biometric Data Specification for Personal Identity Verification, 2007.*

*NIST SP: 800-57 Recommendation for Key Management, March 2007*

*Part 1, General (Revised)*

*Part 2, Best Practices*

*Part 3, Application Specific Key Management Guidance (Draft), October 2008*

## **Configuration Management**

Transportation networks, and especially traffic control systems and field devices, require active configuration and maintenance. As delivered from manufacturers and resellers, default configurations from the manufacturers and vendors are designed for easy deployment, not for security. Network devices may have open services and ports and support for older (vulnerable) protocols. Not only must the systems and devices be secured upon installation, their ongoing management and maintenance needs to be secured as well, and must be capable of managing changes and adapting to new vulnerabilities or the emergence of new threats.

Secure standard configurations one of the *COBIT Critical Controls* First Five or five "quick wins" - "the most effective means yet found to stop the wave of targeted intrusions that are doing the greatest damage to many organizations." *NIST 800-82 Guide to Industrial Control Systems (ICS) Security* summarized the "most successful method for securing control systems" is to gather industry recommended practices and draw on wealth of information available from standards organizational activities.



### **Configuration Management Basics**

- Create and maintain a baseline configuration of information technology and control systems.
- Follow strict configuration management. Security configuration of devices should be documented, reviewed, and approved as consistent with agency cybersecurity policy. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.
- All new configuration rules should be documented and recorded in a configuration management system, with a specific business reason for each change and an expected duration of the need.
- Verify standard device configurations to detect changes. All alterations to such files should be automatically reported to cybersecurity personnel.
- Restrict access to configuration settings and ensure the configuration change control processes are in place.
- Build and maintain a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this secure image should be integrated into the organization's change management processes.

### **Control System Considerations**

- Negotiate contracts to buy systems configured securely out of the box.
- Security settings of IT products should be set to the most restrictive mode consistent with control system operational requirements.
- Ensure that all modifications to control system network meet security requirements identified in risk assessment and mitigation plans.

### **Selected Configuration Management Technical Resources:**

*NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.*

*NIST SP: 800-70, Rev. 3 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers, 2015.*

*NIST SP 800-82 Rev 1, Guide to Industrial Control Systems (ICS) Security, May 13, 2013.*

*NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.*

*Critical Controls for Effective Cyber Defense, 20 Critical Security Controls – Version 4.1, March 2013*

### **Bring Your Own Device (BYOD) Recommended Security Practices**

Replicating traditional cybersecurity policies to address mobile devices and other employee or contractor owned consumer devices – known as Bring Your Own Devices (BYOD) – may be impractical, if not difficult. Privacy is a major concern in consumer owned devices, which

raises the issues of separating agency data from private data. Applying controls to the data rather than the device may be a more practical solution.

There are a number of recommended security practices that address BYOD. *A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (2012)* was developed by based on lessons learned from successful BYOD programs. Management policies and risk assessment have been found to be critical to BYOD cybersecurity.

#### **Bring-Your-Own-Device Cybersecurity Basics**

- Assess and document risks in information security (operating system compromise due to malware, device misuse, and information spillover risks); operations security (personal devices may divulge information about a user when conducting specific activities in certain environments) and transmission security (protections to mitigate transmission interception).
- Consider data sensitivity when reviewing apps in use and conducting a risk assessment. Clarify ownership of the apps and data.
- Identify permitted and supported devices to prevent introduction of malicious hardware and firmware. Recommend an approach to content storage (e.g. cloud vs. device).
- Controls should be applied to the data rather than the device. Set operational principles on the use of allowed cloud services.
- Define content applications that are required, allowed, or banned and consider use of mobile device management (MDM) and mobile application management (MAM) enterprise systems to enforce policies.
- Address app compatibility issues (e.g., accidental sharing of sensitive information due to differences in information display between platforms)
- Keep policies and processes up to date. Employee agreements that address wiping personal and corporate data must be active, not passive, with signatures and human resource record.

#### **Selected BYOD Resources:**

***Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device, Digital Services Advisory Group and Federal Chief Information Officers Council, August 23, 2012***

## Monitoring and Detection

Many resources have cited the importance of monitoring, logging, and analyzing successful and attempted intrusions to systems/networks as a critical component of cybersecurity. These elements are essential to “establishing a continuing process for security improvement”. *APTA Recommended Practice: Securing Control and Communications Systems in Rail Transit Environments Part II* includes a companion concept to Defense-in-Depth - Detection-in-Depth, a “way to detect that an intruder has gained access”. The Practice recommends that detection methods be created for each zone and defensive layer.

It is recommended that anomalies, successful and attempted intrusions, and accidental and unintended incidents be logged and analyzed as part of an ongoing cybersecurity process.

Common monitoring and detection challenges have been identified:

- There is too much data to analyze.
- Too many alerts and false positives occur to effectively identify problems and issues.
- There is incomplete visibility of network and endpoints.

Average time to detect data breach is  
229 days  
Mandiant Threat Report 2014

Average time to detect cybercrime is  
170 days  
Ponemon Institute Report 2014

Average time to detect malicious  
insider is 259 days  
Ponemon Institute Report 2014

Any deficiencies in monitoring, logging and analysis provide opportunities for network compromises and security incidents. Intrusions can be hidden, and are commonly hidden – the average time to detect data breaches and/or a malicious insider is over 200 days. Even when incidents are detected, without protected and complete logging records it is difficult to determine the details of the incident and what effects it has on the network and systems.

Poor or nonexistent log analysis processes allow intrusions such as APTs for months or years without anyone in the organization knowing about it, even though the evidence may be recorded in unexamined log files.

### Monitoring and Detection Basics

- A baseline of network operations and expected data flows for users and systems is established and managed.
- Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. Monitoring of sensors, logs and other network elements should be done on a real-time basis where feasible.
- Detected events are analyzed to understand attack targets/methods and to determine impact of events. Have security personnel and/or system administrators run biweekly reports that identify anomalies. They should then actively review the anomalies, documenting their findings.
- Event data are aggregated and correlated from multiple sources and sensors.
- Incident alert thresholds are established.

- Ensure that the collection system does not lose events during peak activity, and that the system detects and alerts if event loss occurs (such as when volume exceeds the capacity of a log collection system).
- Develop a retention policy to make sure that the logs are kept for a sufficient period of time. Organizations are often compromised for several months without detection. The logs must be kept for a longer period of time than it takes an organization to detect an attack so they can accurately determine what occurred.

#### **Control System Considerations**

- Control systems may not have logging or auditing capabilities or be compatible with IT automatic monitoring tools. Auditing utilities should be tested (e.g. off-line on a comparable control system) before being deployed on an operational system.
- Logs maintained by a control system application may be stored at various locations and may or may not be encrypted.

#### **Selected Monitoring and Detection Technical Resources**

*NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.*

*NIST SP: 800-61, Rev 2, Computer Security Incident Handling Guide, 2012.*

*NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security May, 2015.*

*NIST SP 800-92 Rev 1, Guide to Computer Security Log Management , 2006.*

*NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.*

*Critical Controls for Effective Cyber Defense, 20 Critical Security Controls - Version 4.1, March 2013*

#### **Case Study - Metropolitan Atlanta Rapid Transit Authority (MARTA)**

The Metropolitan Atlanta Rapid Transit Authority (MARTA) operates heavy rail, bus transit, and paratransit services. MARTA's heavy rail system is comprised of four lines including two lines serving the Hartsfield Jackson Airport; its bus operations encompass 91 routes covering one thousand route-miles. MARTA, the ninth largest U.S. transit system in terms of unlinked passenger trips, provided 135 million trips in 2012. (2014 APTA Public Transportation Fact Book)

MARTA used information generated by the CSET® tool along with APTA's Recommended Practice Part 2 to conduct cybersecurity gap analysis and risk assessment. The Cybersecurity Evaluation Tool (CSET®) developed by DHS's Control Systems Security Program assists agencies and asset owners in assessing their cybersecurity practices through a series of detailed questions about components, architecture, policies, and procedures. CSET's Four-Step Process is shown in the diagram below:

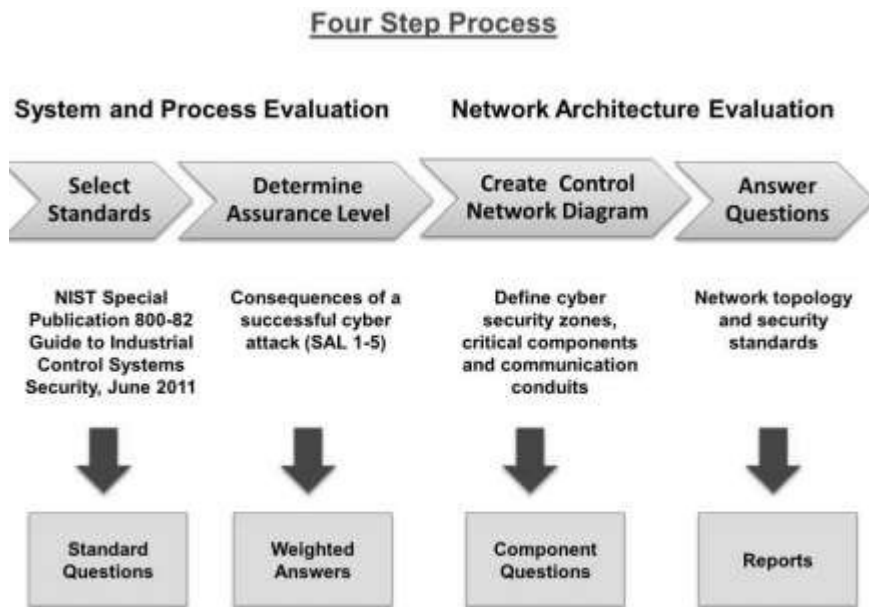


Figure 19: CSET Four Step Process

In December, 2012, the DHS conducted a two-day onsite consultation and assisted MARTA in using CSET. Based on MARTA’s answers to questions on the consequences of a successful cyber attack, Security Assurance Levels (SALs) were determined by the tool. Depending on the SAL, a cybersecurity level to protect against a worst-case scenario was then established. Each component received gap and priority ratings, and on-site and off-site SAL ratings.

A network diagram created with the assistance of the tool helped MARTA staff visualize the criticality of network components and define cybersecurity zones, critical components, and communication conduits. ICS Administrative-level results were reported in the following Table:

**Table 6: ICS Administrative-Level Results**

Administrative	Initial CSET Gaps	Priorities	# Related APTA Controls
Security Policy & Procedures			
Security Program Management			
Configuration Management			
Audit and Accountability			
System Development & Maintenance			
Physical & Environment Security			
Access Control			
System & Information Integrity			
Network Architecture			
System & Communication Protection	0	12	100

Priority = Highest Risk Based on Availability, Probability and Severity

ICS Administrative-level Access Control results identified gaps and were matched with APTA controls. They were then analyzed according to Availability, Probability, and Severity.

The result of the assessment was a 300+ page report with high-level recommendations and observations. MARTA has been prioritizing the recommendations with the assistance of APTA. Recommendation implementation challenges were due to difficulty in replacing or retrofitting legacy systems, and agency resource constraints. MARTA's high-level timeline for its train control and SCADA cybersecurity is shown below:



Figure 20: MARTA Cybersecurity High-Level Timeline

## Chapter 6 Training: Building a Culture of Cybersecurity

### *What is a Culture of Cybersecurity?*

In a security culture, security is an integral part of the daily routine. (*NCHRP Report 793, 2014*) Similarly, a cybersecurity culture is an environment in which cybersecurity best practices are a way of life and essential in ensuring the information security of state transportation agencies and transit agencies. In fact, the first goal of the *Transportation Roadmap (August, 2012)* is to build a cybersecurity culture, and the desired end state of this goal is the merging and integration of cybersecurity and ICS.

Cybersecurity involves People, Technology, and Process. People, essential in the creation of a cybersecurity culture, are often thought to be the most vulnerable element and therefore require significant attention (e.g., training). *NIST SP 800-16 A Role-Based Model for Federal Information Technology/Cybersecurity Training, Revision 1 Third Draft (2014)* emphasizes the importance of the human factor and states “*Federal agencies and organizations cannot protect the integrity, confidentiality, and availability of information in today’s highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them.*”

Culture is fueled by good basic practices which some describe as “cyber hygiene” and sustained awareness by all employees. Cyber Hygiene is essential as many successful breaches typically employ basic techniques. Cybersecurity practices of an employee during their non-working hours can affect work-related cybersecurity. For example, an employee accustomed to using simple passwords may continue this practice for work-related matters. Cyber hygiene practices identified in the literature review included:

- Encouraging staff to follow basic security policies and procedures
- Removing unnecessary application and functions from systems
- Changing default configuration options and passwords

Recent legislation emphasizes the importance of good cybersecurity workforce initiatives. The *Homeland Security Workforce Assessment Act* which was signed into law December, 2014 requires DHS to assess its cybersecurity workforce and create a strategy “*to enhance the readiness, capacity, training, recruitment and retention of its cybersecurity workforce.*”

Many of the elements of the strategy developed through this legislation may be useful in helping state DOTs and transit agencies address their cybersecurity workforce needs.

The development of a cybersecurity culture will also require multi-faceted initiatives which include the following:

- Awareness program
- Training program
- Assessment of threats

- Reduction of the attack surface
- Addressing threats, mitigations, software/firmware update process
- Addressing monitoring and detection methodologies
- Ability to be audited for compliance
- Change-management systems

( *Source: APTA Recommended Practice, Part 2* )

Existing and planned workforce development initiatives of state DOTs and transit agencies include internship or apprenticeship programs and mentorship programs. Internship or apprenticeship programs offer the opportunity for job advancement for individuals without relevant experience by providing on-the-job experience and training. Mentoring programs match more experienced employees with less experienced ones so that the latter may benefit from knowledge and skills of the former. These programs can strengthen cybersecurity culture and encourage young individuals to seek out cybersecurity career paths within the state DOT or transit agency by delineating training milestones and relationship with job advancement.

The culture, once created, must be sustained through continued, heightened focus on good cybersecurity practices and hygiene. Considerable effort may be required to accomplish this due to various demands on the time and resources of senior management and staff.

### ***Importance of Awareness and Training***

The importance of awareness and training with respect to security and safety is well-understood at the federal level and by state transportation agencies and transit agencies. Ensuring that all employees' key issues involved in cybersecurity including the consequences of a cyber breach and their agency's policies regarding the use of IT systems and applications is essential for cybersecurity and the creation of a cybersecurity culture as well. As noted in the literature review, the importance of training is discussed in cybersecurity and information security literature. The *National Rural Electric Cooperative Association Guide to Developing a Cybersecurity and Risk Mitigation Plan* states that

*Insufficiently trained personnel are often the weakest security link in the organization's security perimeter and are the target of social engineering attacks. It is therefore crucial to provide adequate security awareness training to all new hires, as well as refresher training to current employees on a yearly basis.*

The *Transportation Roadmap (August, 2012)* mentions that training and educating agency employees and new hires on cybersecurity is vital. The Roadmap's two near-term training-related objectives include the education of transportation executives on the importance of ICS cybersecurity and the development of a cybersecurity awareness training program.

The *Cybersecurity Framework (Version 1.0, February 12, 2014)* contains an Awareness and



Training category as a component of the Protect function. (The other four functions are Identify, Detect, Respond, and Recover.) The Awareness and Training category description is as follows:

**Awareness and Training:** *The organization’s personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.*

The key principle underlying the Awareness and Training category is that all users need awareness education while certain positions require understanding of their roles and responsibilities necessitating role- and/or responsibility-specific training.

### **Organizational Support**

Organizational support is critical in the development of a cybersecurity culture and should include the allocation of agency resources, senior management leadership and support, and the establishment of appropriate policies and protocols.

First, resources are necessary to implement and maintain cybersecurity awareness and training programs. The required funds need to be programmed into the agency’s multi-year budget and cybersecurity programs into the agency’s strategic plan.

Second, while cybersecurity is every employee’s responsibility, senior management sets the tone and leads by example. They must demonstrate the significance of cybersecurity by being role models and through active engagement in cyber initiatives. They also need to ensure that the required funds are allocated to cybersecurity programs.

Third, cybersecurity incidents need to be identified, reported, and tracked. Agency policies and protocols must be developed in accordance with federal and industry guidance and standards to support these tasks. These policies and protocols then need to be communicated to all agency personnel so that they know how to identify and report a suspicious cyber incident. Those responsible for critical agency infrastructure and assets require additional training and information (including being able to recognize unusual patterns/spikes in incidents and relationships between physical and cyber incidents.)

### **Building upon Safety and Security Cultures**

Model security and safety awareness and training programs and existing workforce programs and initiatives can be used by agencies to facilitate the development and deployment of cybersecurity awareness and training programs.

The tools and initiatives used to construct safety and security cultures within state DOTs and transit agencies can also be used to establish a cybersecurity culture.

Over the past few decades, transit agencies have succeeded in building a culture of safety and ingraining safety into the mindsets of transit employees. As stated in *APTA Recommended Practices, Part 2*, “[j]ust as transit agencies have created a safety-centric culture-saving lives and reducing accidents and accident severity-they need to foster and create a cybersecurity culture.” State DOTs have also developed or are in the process of

developing comprehensive safety programs.

Because transit systems around the world have been targets of terrorists, security was a concern for senior management of transit agencies even prior to September 11, 2001. After the terrorist attacks on U.S. soil on 9/11, transit agencies stepped up their efforts to establish a security culture with the support of FTA and DHS/TSA and relevant legislation. For example *Section 1408, PL 110-53; 121 Stat. 266* directed the DHS Secretary to develop/issue regulations for a security training program. *APTA Recommended Practice on Security Awareness Training for Transit Employees (2012)* provides minimum guidelines for security awareness training and implemented security awareness and training programs. These actions helped ensure that all transit employees understood the important role that they play in the security of their transit operations.

A national security awareness program – “If You See Something, Say Something®” – which was initially developed by the MTA in the New York metro area and the Transit Watch program initiated in 2003 by the FTA that was operated as a partnership with APTA, ATU and DHS may be used as models of successful coordinated approaches to disseminate content and raise and maintain awareness of transit and state DOT employees. The campaigns used a variety of information dissemination techniques and media including video, posters, TV and radio advertisements, etc.

### ***Cybersecurity Awareness and Training Program***

The *Federal Information Security Modernization Act (2014)* - formerly the Federal Information Security Management Act (FISMA) - governs federal IT and cybersecurity and requires role-based training for federal personnel and other users of federal IT systems. The 2014 FISMA gives DHS authority over government-wide IT operations and management of day-to-day security issues while OMB retains budgetary authority and responsibility for cybersecurity policies for information security within federal agencies. Both agencies are expected to coordinate with NIST and comply with NIST standards and guidance.

The required information security program needs to include:

- Periodic risk assessments, determination of the risk and magnitude of potential harms, and the development of countermeasures to reduce the information security risks to acceptable levels.
- Security awareness training to inform personnel including contractors and other users regarding information security risks associated with their activities and their responsibilities in complying with agency policies and procedures.
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices no less than annually; the testing includes “management, operational and technical controls of every information system” in the section 3505(c) inventory and may include testing for the evaluation under section 3555.

As new guidance for the 2014 FISMA is developed, state DOTs and transit agencies may benefit from consulting the guidance in addition to guidance and regulations of USDOT, FHWA, FTA, and other regulatory agencies in establishing cybersecurity awareness and training programs.

It is important to note the differences between Awareness and Training. *NCHRP Report 793* states that “*security awareness is the cornerstone of a security culture.*” *NIST SP 800-16* notes that “*Awareness is not training. The purpose of awareness presentations is simply to focus attention on security.*” *NIST SP 800-50* describes awareness efforts as “*designed to change behavior or reinforce good security practices.*” Having sustainable processes and methods is noted in *NCHRP Security 101* as a key objective of a security awareness program.

While Awareness focuses attention on specific issues with the learner as a passive recipient of information, Training requires the participation of the learner to generate security skills and competencies. (*NIST SP 800-50, 2003*) Those who require more specialized knowledge of IT and cybersecurity will pursue education which integrates relevant skills and competencies into a common body of knowledge.

In NIST’s cybersecurity learning continuum model, learning progresses from security awareness to cybersecurity essentials to role-based training to education and/or experience. The Cybersecurity Essentials is a new element that was added to the continuum.

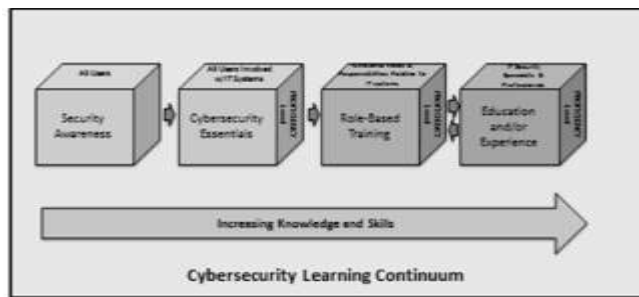


Figure 21: Cybersecurity Learning Continuum. Source: NIST SP 800-16, Revision 1 (Third Draft) October, 2014

The four key elements of the continuum shown in Figure are summarized below:

1. “Security Awareness” applies to all employees, focuses attention on cybersecurity and cybersecurity issues, and helps employees recognize and respond to the issues. (page 27- 29)
 

“Cybersecurity Essentials” is introduced in the revised NIST SP 800-16 as a foundation of knowledge needed for employees and contractors having access to IT systems to protect electronic information and systems. (page 29)
2. Cybersecurity essentials include:
  - Technical underpinnings of cybersecurity and its taxonomy, terminology and challenges;
  - Common information and computer system security vulnerabilities;
  - Common cyber attack mechanisms, their consequences and motivation for use;
  - Different types of cryptographic algorithms;
  - Intrusion, types of intruders, techniques and motivation;
  - Firewalls and other means of intrusion prevention;

- Vulnerabilities unique to virtual computing environments;
3. “Role-Based Training” delivers the knowledge and skills required for specific roles and responsibilities with respect to Federal Organization information systems. Competency differences among users are recognized.

*NIST SP 800-16 Role-Based Model for Federal Information Technology/Cybersecurity Training* describes how to train the Federal workforce that have significant IT/cybersecurity responsibilities. FIPS publications including *FIPS 200 Minimum Security Requirements for Federal Information and Information Systems* and *FIPS 199 Standards for Security Categorization of Federal Information and Information Systems* and NIST publications such as *NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems*, *NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*, *NIST SP 800-18 Guide for Developing Security Plans for Federal Information Systems*, and *NIST SP 800-50 Building an Information Technology Security Awareness and Training Program* are implementers.

*NIST 800-50* provides guidance on conducting needs assessments which is the first step in creating role-based training. Needs assessments help to identify roles that require training and training gaps. The second step, functions identification, may be found in *NIST 800-16, Appendix A, Functions Appendix*. The third step is to fill-in the associated outcomes and learning objectives. See Appendix B and C of *NIST 800-16* for guidance on establishing the objectives, and knowledge and skills for specific roles. The trainer can then adjust modules according to the expertise of the learners.

4. “Education” develops the ability and vision for complex and multi-disciplinary tasks and tracking changes to the threat and technology environments. Education is attained through experience, cooperative training, certification and advanced education. (page 31- 34)

According to *NIST SP 800-50 (2003)* prior to the development of a cybersecurity Awareness and Training Program, the following steps should be taken:

- Conduct a needs assessment
- Develop a strategy
- Complete an awareness and training program plan for strategy implementation
- Develop awareness and training material
- Address funding issues
- Communicate plan and its benefits to senior management and support personnel

Three possible models of the program are described in *NIST SP 800-50 (2003)*. All three have a centralized policy but can have centralized or distributed strategy as well as centralized or distributed implementation. The model that is selected depends on size and geographic dispersion of the organization, organizational roles and responsibilities, and budget allocations and authority.

- Model 1 – Centralized policy, strategy, and implementation
- Model 2 – Centralized policy and strategy, distributed implementation

- Model 3 – Centralized policy, distributed strategy and implementation

*NIST SP 800-50 (2003)* also discusses how to structure awareness and training activity; how to conduct a needs assessment; how to develop an awareness and training plan; how to establish priorities; how to establish the level of complexity of the subject matter; and how to fund the program. Guidance on evaluating and testing training and exercise programs are found in *NIST SP 800-84 and SP 800-16*.

New legislation enacted in December, 2014, the *Cybersecurity Enhancement Act*, intends to direct the NIST to further support the 2014 *Cybersecurity Framework* likely through updates and improvements to the existing Framework.

### **Functions and User Categories**

While training needs of transit employees depend on agency position functions and responsibilities, all employees require understanding of basic cyber awareness because they may have access to an agency PC, laptop, or mobile device or bring their own device to work. Vendors and contractors would also benefit from the agency's awareness program.

When any transit employee as well as vendors and contractors connect to any part of the network or to any device using any means, they should be aware of basic precautions that should be taken. When any suspicious email or incident occurs, the transit employee needs to be able to detect and observe it, and report it to the proper staff. In most cases basic users need to know when and to whom an incident should be reported but may not need to decide on a course of action or respond to an incident; however, in rare cases in which a cyber breach causes life safety concerns, basic users will need to know what actions they must take.

In the typical agency, ICS is the responsibility of engineering and operations personnel but IT is responsible for cybersecurity plan(s) and their implementation. Both units need to work together to create and implement the plan(s) and understand their respective roles and responsibilities. Hence, including personnel from both units in awareness and training activities will enhance interaction and cooperation between the units.

Those with lead responsibility need the latest guidance and standards, compliance requirements, and know how to meet them.

- The OPM requires users to receive cybersecurity awareness and training on rules and responsibilities prior to accessing IT systems and applications. OPM also requires training for Current employees including IT management and operations personnel; Coos, IT program managers, auditors, and other IT personnel; program and functional managers; executives
  - New employees within 60 days of hire
  - When employees start a new position that requires additional role-specific training
  - Whenever there is a change in the IT security environment or procedures
  - Periodically as refresher training

The following user categories are derived from the *Cybersecurity Framework (Version 1.0, February 12, 2014)*. All users should understand their roles and responsibilities. The Framework also identifies five high-level functions - Identify, Protect, Detect, Respond,

and Recover. Each category of user is responsible for all five functions to varying extents.

**All Users** should be informed about agency cybersecurity policies and protocols and receive basic awareness content. Users are individuals requiring access to the agency's electronic information or systems and "are the single most important group of people who can help reduce unintentional errors and related information system vulnerabilities." (*NIST 800-16 Revision 1 Third Draft, 2014*) Users should understand and comply with IT/cybersecurity policies and procedures. They refer to all categories of personnel including frontline employees, supervisors, maintenance workers, and administrative and support staff.

**Third-Party Stakeholders** include suppliers, vendors, partners, and customers.

**Privileged Users** are "authorized (and, therefore, trusted) to perform functions that ordinary users are not authorized to perform." (2014 Cybersecurity Framework) Therefore, it is important for privileged users to fully understand their roles and responsibilities.

**Managers and Senior Executives** are responsible for complying with and emphasizing the importance of IT/Cybersecurity role-based training requirements. Senior Executives are grouped into a separate category of users in the Cybersecurity Framework as they have greater decision-making roles and responsibilities. The Chief Information Officer (CIO) has overall responsibility to administer training and oversee personnel with IT/cybersecurity responsibilities.

**Training Personnel** seek to deliver necessary training and education to achieve desired awareness levels and understanding of roles and responsibilities. Training personnel also monitor and evaluate the overall effectiveness of the Awareness and Training program as well as individual courses and sessions. The Senior Agency Information Security Officer (SAISO) has tactical-level responsibility for the cybersecurity training and awareness program including its implementation. The Cybersecurity Training Manager/Chief Learning Officer (CLO) is responsible for specific role-based training. The Training Developer/Instructional Design Specialists assist in the development of role-based training materials.

**IT/Cybersecurity Personnel** have a significant impact on the success of IT/cybersecurity awareness and training programs and require more specialized knowledge of IT/cyber systems. They also assist in the design and development and review and evaluation process and procurement of systems and equipment. IT/Cybersecurity personnel include:

- Information Technology (IT) Personnel
- Technologists
- System Administrators
- Control System Operators
- System Architects
- Other Personnel with IT/Cybersecurity Responsibilities

**Physical Security Personnel** include in-house and external police and security and local law enforcement. Physical Security Personnel should be aware of cybersecurity issues and impact of cyber breaches on physical assets and infrastructure as well as the consequences of physical breaches on IT systems. Coordination between physical security and cybersecurity

personnel is pertinent in ensuring the security of agency CIKR.

## **Content**

A Cybersecurity Awareness and Training Program should cover IT security policies and procedures, rules of behavior for IT systems and information use, basic threats employees may encounter and actions that they should employ to counter them. Issues include whether the training content will be developed in-house or outsourced. Considerations include availability of resources and staff with adequate skills, cost, content sensitivity, and training schedules. As noted in *NIST SP 800-50 (2003)*, canned presentations are impersonal and interest in the training may be lost. Therefore, adapting the content to the audience will assist participants in understanding the relevance of the material to their daily work and how it can be integrated into their roles. The three key training areas identified in *NIST SP 800-16* are Laws and Regulations, Security Program, and System Life Cycle Security. The IT Security Training Matrix in *NIST SP 800-16* maps the three training areas to employee functions.

### **Awareness Content**

The objective of Awareness activities is to enhance recognition and retention of information. The following topics may be appropriate for Awareness content:

- Ability to recognize potential threats including social engineering attempts
- Ability to differentiate between real and fake messages
- Ability to respond appropriately and report an incident
- Knowing when and how to report an incident
- Understanding record-keeping procedures
- Understanding effective password management techniques
- Understanding agency policy on agency mobile phone and tablet security/use
- Understanding agency policy on personal mobile phone and table security/use
- Understanding the implications of security breaches

*(Source: NIST SP 800-16, NIST SP 800-50)*

Awareness content should be updated on a regular basis. Possible sources include NIST Special Publications, APTA Recommended Practices, IT news sources and advisories, professional organizations, conferences and workshops, courses, agency audits and assessments.

### **Training Content**

Key high-level cybersecurity functions have been identified in the *2014 Cybersecurity Framework*. They are: Identify, Protect, Detect, Response, and Recover. Elements (categories) of each of these functions are presented in the following Table.

While Awareness and Training resides in the “Protect” function, required training should to be aligned with each of these elements (categories).

**Table 7: Cybersecurity Functions, Elements and Categories**

<b>FUNCTION</b>	<b>ELEMENTS/CATEGORIES</b>
IDENTIFY	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
PROTECT	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
DETECT	Protective Technology
	Anomalies and Events
	Security Continuous Monitoring
RESPOND	Detection Processes
	Response Planning
	Communications
	Analysis
	Mitigation
RECOVER	Improvements
	Recovery Planning
	Improvements
	Communications

Source: 2014 Cybersecurity Framework (Version 1.0, February 12, 2014)

Resources for training content are provided in the Appendix. Additional resources are expected to be developed as mandated in the new cybersecurity legislation. Training content obtained from these sources may need to be adapted to the requirements of the agency.

*NIST SP 800-16 Appendices* contain helpful information on function areas, knowledge and skills, and roles. Appendix A provides information on Function Areas including a general description of the area and the Learning Objectives for each function. Appendix B contains the Knowledge and Skills Catalog and Appendix C presents the roles matrix using generic roles and titles. Appendix C assists agencies in identifying the competencies, knowledge, knowledge unit, and skills required for specific roles. Generic module outlines and corresponding Knowledge and Skills tables are included in the Appendix. The Knowledge and Skills tables categorize information into four functional perspectives – Manage, Design, Implement, and Evaluate. Knowledge is defined as “the theoretical or practical understanding of the competency.” A Knowledge Unit is the set of competencies associated with a role. A sample module and corresponding table are presented below.



INFORMATION TECHNOLOGY/  
CYBERSECURITY TRAINING  
Module for Roles

**Function Area:** Operate and Maintain

**Role Area:** Data Administration

**Roles:**

- Data Security Analyst
- Data Management Systems Security
- Data Administrator
- Database Administrator
- Content Staging Specialist
- Data Architect
- Data Manager
- Data Warehouse Specialist
- Database Developer
- Information Dissemination Manager
- Information System Integrator

**Responsibility** — Develop and administer databases and/or data management systems that allow for the storage, query, and utilization of data.

**Knowledge Unit:**

- Data Security
- Digital Forensics
- Database
- Cryptography and Encryption
- Architecture
- Identity Management/Privacy
- Information Systems
- Modeling and Simulation
- Incident Management

Figure 22: Sample Training Module

**Table 8: Sample Training Knowledge and Skills****Corresponding Knowledge and Skills**

Knowledge Unit	All	Manage	Design	Implement	Evaluate
<b>Data Security</b>	DS-2 DS-10 DS-18	DS-4	DS: 3 - 8 DS: 13 - 14 DS: 16	DS: 3 - 6 DS-9 DS-12 DS: 17-18	DS-9 DS-11 DS-13 DS-15 DS: 17-18
<b>Digital Forensics</b>				DF-6	DF-7 DF-31
<b>Database</b>		DB-5	DB-1 DB-2 DB-4 DB-6	DB-3 DB: 7 - 8 DB: 9 - 11	
<b>Cryptography and Encryption</b>		CR-10 CR-12	CR-1 CR-5	CR-3 CR-5 CR-7	CR-9
<b>Architecture</b>		ARCH-15	ARCH-2 ARCH-7 ARCH: 18 – 21	ARCH-1 ARCH-3 ARCH-4 ARCH-9	
<b>Identity Management /Privacy</b>	IM: 1-3 IM-7	IM-9 IM-11	IM-5	IM: 4-6 IM-9	IM-4 IM-5 IM-8 IM-10 IM-11
<b>Information Systems</b>	SI: 1-3 SI-10 SI: 27 -28 SI-30	SI-25	SI-4 SI-5 SI-9 SI-13 SI-25 SI-29	SI-5 SI-7 SI-8 SI-9 SI: 14 - 15 SI-20 SI-25 SI-29 SI-31	SI-17 SI-26 SI-31
<b>Modeling and Simulation</b>			MS: 2 – 3		
<b>Incident Management</b>	IR-20	IR-2 IR-3 IR-6 IR-14 IR-16 IR-18		IR-4 IR-12	IR: 2 - 3 IR-14

**Awareness and Training Delivery**

Existing programs may be useful for the delivery of cybersecurity awareness and training. Agencies that offer a security awareness course may choose to incorporate a cybersecurity awareness module into the course. Those that offer tuition reimbursement programs may incorporate cybersecurity training into their programs. Agencies that have existing partnerships with other state DOTs or transit agencies, colleges, universities, LTAP/TTAP or RTAP centers, or with other organizations can leverage these partnerships for the provision of cybersecurity training. Some transit agencies have partnerships with transit unions; these and other partnerships and organization may also be leveraged.

Techniques should be aligned with available agency resources and the length and complexity of the messages. Communications strategies for awareness messages include the following:

- Senior management can include security awareness in all of their communications to their employees.
- Managers and supervisors can talk about security at meetings and events.
- Security topics can be discussed at the small unit level.
- Awareness messages may be attached to regular agency newsletters, emails, paychecks, reports, etc. or disseminated through posters, reminder sheets, and employee wallet cards.
- Security awareness can be incorporated via short modules into new or existing training, or into position-specific training. Or, employees may be directed to the FEMA or DHS training materials.

*(Source: NCHRP Report 793, Section 4, 2014)*

NIST provides more specific guidance on delivery of awareness material in ***NIST SP 800-50 Building An Information Technology Security Awareness and Training Program***. NIST recommendations include the following:

- Posters, “do and don’t lists,” or checklists
- Screensavers and warning banners/messages
- Newsletters
- Desk-to-desk alerts
- Agency wide e-mail messages
- Videotapes
- Web-based sessions
- Computer-based sessions
- Teleconferencing sessions
- In-person, instructor-led sessions
- IT security days or similar events
- “Brown bag” seminars
- Pop-up calendar with security contact information, monthly security tips, etc.
- Mascots
- Crossword puzzles
- Awards programs

*(Source: Section 5.2, NIST SP 800-50, 2003)*

Training implementation is particularly difficult for frontline personnel. The ***NCHRP Synthesis Report 468 on Interactive Training for All-Hazards Emergency Planning, Preparation, and Response for Maintenance & Operations Field Personnel (2015)*** described the training delivery issues for frontline personnel whose schedules are usually inflexible – training typically requires overtime or “backfill” pay expenditures. Limited budgets and resources are an issue such as the lack of qualified training staff and inadequate resources. Other impediments included insufficient information about available training, lack of “mandate” and senior management support, distance issues, union-management issues, and employee turnover. Employee turnover has been an issue for agencies as well since turnover causes increased new-hire training needs. At the same time, a quality-training program can help mitigate

turnover issues by improving workforce commitment to the organization.

Interactive training solutions have been identified and discussed in *NCHRP Synthesis Report 468 (2015)*. Technologies such as CCTV, web cams, voice over internet protocol (VOIP), Skype, and web chat apps can be used by agencies with dispersed personnel to deliver quality training.

Shared resource models and inter-jurisdictional and interagency training activities make the most use of scarce resources through the use of common training content and delivery of training to personnel from multiple agencies and jurisdictions. Examples of shared resource models include

- Keystone Transit’s Transit Career Ladder Partnership between SEPTA and Transport Workers Union (TWU) is an example of a successful initiative undertaken by management and the union. The partnership addresses skill and worker shortages and the introduction of new technologies through curriculum development, incumbent worker training, new hire recruitment/training, and assessment. This statewide partnership approach began in Southeastern Pennsylvania with SEPTA and TWU, and then expanded to include smaller regional and local agencies and unions across the state. Additional partner organizations included the Community Transportation Development Center, Amalgamated Transit Union (ATU), the Pennsylvania AFL-CIO, community organizations and training providers.
- Santa Clara Valley Transportation Authority (VTA) Joint Workforce Investment (JWI) Program was a joint labor-management partnership between VTA and the ATU. The JWI included three programs – Maintenance Career Ladders Training Project, New Operator/Mentor Pilot Project, and Health and Wellness project. The Maintenance Career Ladders Training Project addressed mechanic shortages by creating mechanic trainee positions. The New Operator/Mentor Pilot Project provided new operators with mentoring on customer service and stress-coping skills by exemplary operators who had been trained by a local university.

(Source: *NCHRP Report 685 Strategies to Attract and Retain a Capable Transportation Workforce, 2011*. *NCHRP Report 693. Attracting, Recruiting and Retaining a Skilled Staff for Transportation Systems Operations and Management, 2012*. *TCRP Report 162 Building a Sustainable Workforce in the Public Transportation Industry – A Systems Approach, 2013*.)

## **Evaluation**

Evaluation of training helps employees and their supervisors assess their on-the-job performance, trainers to improve the training process including content and delivery, and senior management to better allocate resources. Evaluations measure learning conditions and learner’s perceptions about the training; what a student has learned; outcomes in terms of behavior/performance; and value of the training compared with other options.

*NIST SP 800-84* notes that tests, training, and exercises are developed and implemented to help maintain contingency and incident response plans in a “state of readiness.” (Page ES-1, *NIST SP 800-84, 2006*) It is essential to have plans that are validated through tests and exercises, personnel that have been trained on how to fulfill their roles and responsibilities,

and systems and components tested for their operability. *NIST SP 800-84* denotes training as a vehicle for informing and training personnel on their roles and responsibilities within IT plans and preparing them for participation in tests and exercises.

**Tests** – tests are used to evaluate the operability of systems or components including specific cybersecurity measures. Unannounced tests may be used to test employee behavior. For instance, selected personnel may be subjected to social engineering attempts. Personnel that do not respond appropriately to the attempts may be designated for additional cyber training. For ICS testing of new components is essential to ensure that there are no unintended operational impacts. Tests are conducted in the operational environment or as close to it as possible. Appendix C of the *NIST SP 800-84* presents the following sample documentation for component, system, and comprehensive tests.

- Test structure description
- Test plan
- Test briefing for participants
- Test inject or action
- Test validation worksheet
- Test evaluation worksheet
- Test after action report

**Exercises** – Exercises have been used to validate and improve emergency response plans, allow personnel opportunity to practice what they have learned, and agencies to evaluate team and individual performance. Exercises can help evaluate training effectiveness and identify training needs and gaps. Exercises may be categorized into Discussion-based exercises and Operations-based exercises. Discussion-based exercises (seminars, workshops, tabletop exercises (TTXs), and games) help participants develop as well as understand their roles and responsibilities with respect to new, plans, policies, agreements, and procedures. Operations-based exercises - drills, functional exercises (FEs), and full-scale exercises (FSEs) - are conducted in a simulated operational environment and “validate plans, policies, agreements, and procedures; clarify roles and responsibilities; and identify resource gaps.” (Page 2-5, *HSEEP, 2013*)

Further information on exercise types, their differentiating features, their development and conduct, and evaluation methods can be obtained from the Homeland Security Exercise and Evaluation Program (HSEEP) and the *NCHRP Synthesis Report 468 on Interactive Training for All-Hazards Emergency Planning, Preparation, and Response for Maintenance & Operations Field Personnel*. *NIST SP 800-84* highlights the Tabletop Exercise (TTX), a Discussion-based exercise held in a classroom setting and a Functional Exercise (FE), an Operations-based exercise. The *NIST SP 800-84* Appendix A includes sample documentation for a TTX and Appendix B provides the sample documentation including sample scenarios and exercise injects for a Functional Exercise.

Evaluation results of tests and exercises are summarized in the After Action Report (AAR). The AAR captures lessons learned, other observations, and recommendations, and can result in updates to the IT plan or other documents, briefings, and additional training. *NIST SP 800-84* Appendices provide relevant AAR templates, forms, and information on the conduct of tests, Tabletop Exercises, and Functional Exercises.

## **Performance Indicators**

Indicators may be used to track and evaluate the performance of the Awareness and Training Program. Indicators may be intermediate indicators that describe the output of the program such as the number of trained personnel or they may be outcome indicators that reflect to what extent the program is meeting its goal(s).

Possible intermediate and outcome indicators include percentage of users undergoing awareness training, percentage of those needing role-based training undergoing the training, percentage undergoing recommended refresher training, training delivery rate or number, incident rate, IT policy compliance rate, gap between funding and funding needs, and gap between available skilled personnel and personnel needs. (*NIST SP 800-50, 2003*)

## **Continuous Improvement**

Monitoring the implementation and performance of the program is important in assisting decision makers and others in understanding the effectiveness of program activities. Awareness and Training Program content needs to be updated regularly to address any gaps identified in the performance monitoring process and address technology and other changes.

Supervision can help in the continuous improvement process by monitoring the Cyber Hygiene of their subordinates. For example, if an employee leaves their password on a notepad, their supervisor may instruct the employee not to do so and provide him or her with cybersecurity awareness material. For comprehensive evaluation techniques refer to *NIST SP 800-16*.

## **Awareness and Training Resources**

The cybersecurity content provided in this Section and other Sections of this Guide may serve as the basis for Cybersecurity training.

Two national initiatives are the National Initiative for Cybersecurity Careers and Studies (NICCS) and The National Initiative for Cybersecurity Education (NICE).

The National Initiative for Cybersecurity Careers and Studies (NICCS) is a national resource on cybersecurity awareness, education, careers, and workforce development opportunities. Previously developed cybersecurity courses or modules can also be accessed via this resource.\ online at <http://niccs.us-cert.gov>

The National Initiative for Cybersecurity Education (NICE) is being led by NIST with the cooperation of 20+ federal departments and agencies. The goal of NICE is a national cybersecurity education program for the development and use of sound cyber practices by federal employees, civilians, and students, and includes the following three components:

- Component 1: National Cybersecurity Awareness (Lead: Department of Homeland Security (DHS))
- Component 2: Formal Cybersecurity Education (Co-Lead Department of Education (DoED) and National Science Foundation (NSF))
- Component 3: Cybersecurity Workforce (Lead: DHS, OPM, DoD, DOL)

NICE developed the National Cybersecurity Workforce Framework which defines and categorizes the cybersecurity workforce through common taxonomy and lexicon. Thirty-two specialty areas are grouped into one of seven categories; also, the knowledge, skills, and abilities for each area are provided in the Framework.

*NIST SP 800-16 (1998)* provides the IT security learning continuum model including 26 roles and role-based matrices and 46 training matrix cells, terms and concepts for IT security literacy, training content categories, and functional specialties. *NIST SP 800-50 Building an Information Technology Security Awareness and Training Program (2003)* describes the life cycle of a cybersecurity awareness and training program. The life cycle includes needs assessment and an implementation strategy,

DHS through its ICS-CERT program offers cybersecurity control systems courses. The DHS ICS-CERT Control Systems Security Program (CSSP) can be accessed through the following link - ICS-CERT Virtual Learning Portal <https://ics-cert-training.inl.gov/>

The ICS-CERT program offers varying levels of cybersecurity courses. The CSSP series of ICS cybersecurity courses starts with an introductory course and culminates with a five-day, advanced capstone exercise.

- Instructor Led Format—Introductory Level
- Introduction to Control Systems Cybersecurity (101)—1 day or 8 hrs
- Instructor Led Format—Intermediate Level
- Intermediate Cybersecurity for Industrial Control Systems (201)—1 day or 8 hrs
- Hands-On Format—Intermediate Level
- Intermediate Cybersecurity for Industrial Control Systems (202), with lab/exercises—1 day or 8 hrs
- Hands-On Format—Technical Level
- ICS Cybersecurity (301)—5 days

FEMA EMI offers an Independent Study course, “IS-0523 Resilient Accord—Exercising Continuity Plans for Cyber Incidents.” FEMA also has a resident workshop entitled “E0553 Resilient Accord Cybersecurity Planning Workshop” and a Virtual Tabletop Exercise with a Cyber Focus available to a limited number of participants.

*NIST SP 800-16* Appendices contain helpful information on function areas, knowledge and skills, and roles. Appendix A provides information on Function Areas including a general description of the area and the Learning Objectives for each function. Appendix B contains the Knowledge and Skills Catalog and Appendix C presents the roles matrix using generic roles and titles.

In addition to the TCRP and NCHRP publications and projects already cited in this Chapter, TCRP F-series projects on workforce development contains various strategies and tips for addressing recruitment, retention, professional development, and related workforce needs of transit personnel. *NCHRP Report 693* presents strategies and resources to attract, recruit, and retain transportation system operations and management (SOM) staff and *NCHRP Report 685 on Strategies to Attract and Retain a Capable Transportation Workforce* discusses recruitment and retention topics.

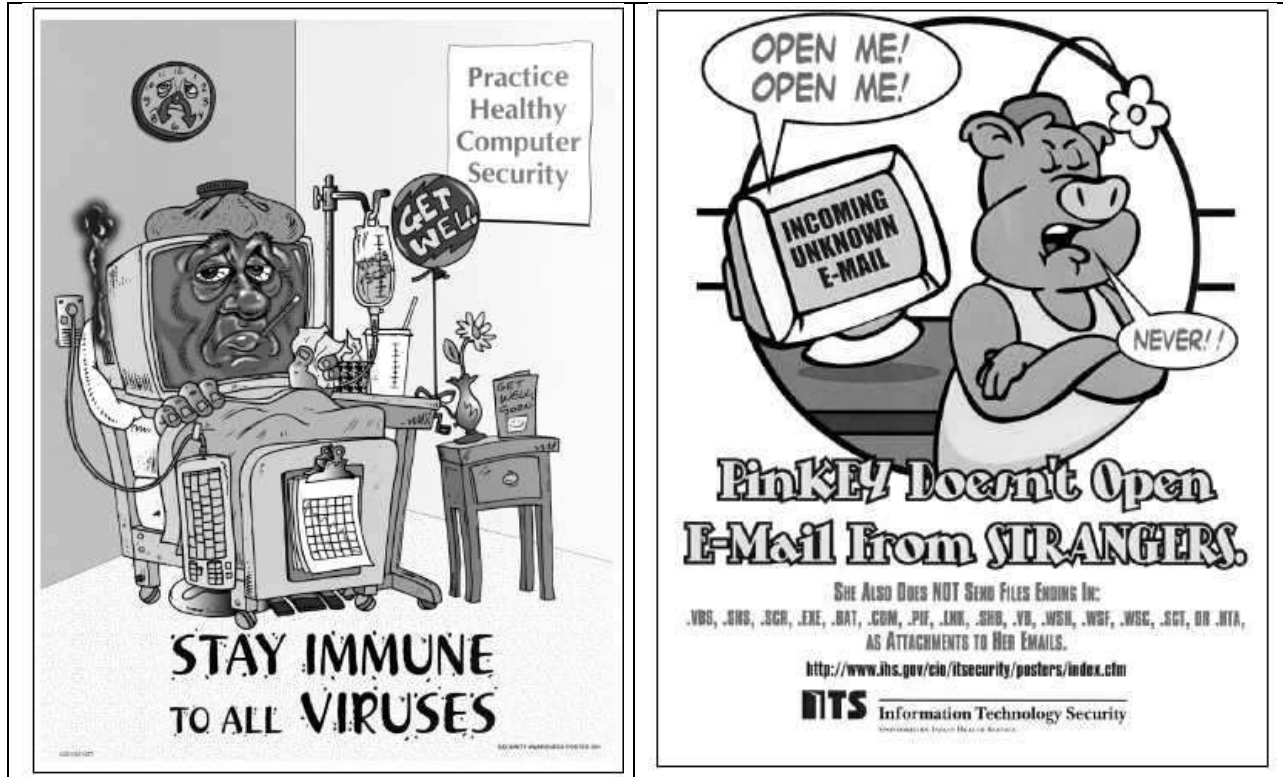


Figure 23: Sample Awareness Posters. Source: NIST SP 800-50, 2003



**Figure 24: Sample Awareness and Training Program Template**

<b>EXECUTIVE SUMMARY</b>
<b>BACKGROUND</b> <ul style="list-style-type: none"> <li>↳ OMB A-130, Appendix III</li> <li>↳ Federal Information Security Management Act (FISMA)</li> <li>↳ Specific department and/or agency policy (and other relevant information or rationale that may drive an awareness and training program and plan)</li> </ul>
<b>AGENCY IT SECURITY POLICY</b> <ul style="list-style-type: none"> <li>↳ Goals</li> <li>↳ Objectives</li> <li>↳ Roles/Responsibilities</li> </ul>
<b>AWARENESS</b> <ul style="list-style-type: none"> <li>↳ Audience (management and all employees)</li> <li>↳ Activities and target dates</li> <li>↳ Schedule</li> <li>↳ Review and updating of materials and methods</li> </ul>
<b>TRAINING/EDUCATION</b> <ul style="list-style-type: none"> <li>Role 1: Executives and Managers                     <ul style="list-style-type: none"> <li>↳ Learning Objectives</li> <li>↳ Focus Areas</li> <li>↳ Methods/Activities</li> <li>↳ Schedule</li> <li>↳ Evaluation Criteria</li> </ul> </li> <li>Role 2: IT security staff                     <ul style="list-style-type: none"> <li>↳ Learning Objectives</li> <li>↳ Focus Areas</li> <li>↳ Methods/Activities</li> <li>↳ Schedule</li> <li>↳ Evaluation Criteria</li> </ul> </li> <li>Role 3: System/Network Administrators                     <ul style="list-style-type: none"> <li>↳ Learning Objectives</li> <li>↳ Focus Areas</li> <li>↳ Methods/Activities</li> <li>↳ Schedule</li> <li>↳ Evaluation Criteria</li> </ul> </li> <li>... and remaining roles with significant IT security responsibilities</li> </ul>

<p><b>PROFESSIONAL CERTIFICATION</b></p> <p>Role 1: IT security staff</p> <ul style="list-style-type: none"> <li>↳ Learning Objectives</li> <li>↳ Focus Areas</li> <li>↳ Methods/Activities</li> <li>↳ Schedule</li> <li>↳ Evaluation Criteria</li> </ul> <p>Role 2: System/Network Administrators</p> <ul style="list-style-type: none"> <li>↳ Learning Objectives</li> <li>↳ Focus Areas</li> <li>↳ Methods/Activities</li> <li>↳ Schedule</li> <li>↳ Evaluation Criteria</li> </ul> <p>... and remaining roles with significant IT security responsibilities</p>	
<b>RESOURCE REQUIREMENTS</b>	<b>COST</b>
↳ Staffing	\$ xxx
↳ Contracting Support	\$ xxx
↳ Facilities (e.g., training rooms, teleconferencing facility)	\$ xxx
↳ Media (e.g., server(s) for web- and computer-based material)	\$ xxx

**Table 9: Awareness and Training Subcategories and References**

Awareness and Training Subcategories	References
All users are informed and trained	CCS CSC 9 COBIT 5 APO07.03, BAI05.07 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.7.2.2 NIST SP 800-53 Rev. 4 AT-2, PM-13
Privileged users understand roles and responsibilities	CCS CSC 9 COBIT 5 APO07.02, DSS06.03 ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 AT-3, PM-13
Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	CCS CSC 9 COBIT 5 APO07.03, APO10.04, APO10.05 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2 NIST SP 800-53 Rev. 4 PS-7, SA-9
Senior executives understand roles and responsibilities	CCS CSC 9 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, NIST SP 800-53 Rev. 4 AT-3, PM-13
Physical and information security personnel understand roles and responsibilities	CCS CSC 9 COBIT 5 APO07.03 ISA 62443-2-1:2009 4.3.2.4.2 ISO/IEC 27001:2013 A.6.1.1, A.7.2.2, NIST SP 800-53 Rev. 4 AT-3, PM-13

Source: 2014 Cybersecurity Framework (Version 1.0, February 12, 2014)

## Chapter 7 Security Programs and Support Frameworks

To assist in the protection of transportation infrastructure, the federal government has issued a number of legislative initiatives, presidential orders, and federal department mandates, regulations, and guidelines. This chapter identifies components of the federal government's infrastructure protection and cybersecurity strategies that relate to the transportation sector. Through understanding these initiative and activities, transportation agencies can obtain a sense of the national strategies and supportive frameworks available to help them in reducing cybersecurity risks.

### **Cybersecurity and Critical Infrastructure**

The *USA Patriot Act of 2001* (P.L.107-56) established the federal definition of “critical” infrastructure still in use today:

*Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Sec. 1016(e)).*

*The National Strategy To Secure Cyberspace*, issued in early 2003, outlined priorities for protecting against cyber threats and the damage these threats can cause. The Strategy called for DHS and the Department of Energy (DOE) to work with industry to

*... develop best practices and new technology to increase security of digital control systems/SCADA systems, to determine the most critical digital control systems/SCADA-related sites, and to develop a prioritized plan for short-term cybersecurity improvements in those sites.*

*Presidential Policy Directive 8: National Preparedness*, issued in 2011, to strengthen security and resilience through five preparedness mission areas—Prevention, Protection, Mitigation, Response, and Recovery – includes cyber in its national preparedness goals.

*Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments.*

*The National Infrastructure Protection Plan (NIPP) and its complementary Sector-Specific Plans (SSP)*, which provide a unifying structure for integrating current and future CI/KR protection efforts, recognizes that the U.S. economy and national security are highly dependent upon the cyber infrastructure. The NIPP 2013 evolves the concepts introduced in the initial 2006 version that was then revised in 2009. The 2013 National Plan

*provides the foundation for an integrated and collaborative approach to achieve the vision of: “[a] Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened.*

**Executive Order 13636 (EO) Improving Critical Infrastructure Cybersecurity**, issued in February 2013, calls for the development of a voluntary Cybersecurity Framework that provides a “prioritized, flexible, repeatable, performance-based, and cost-effective approach” for assisting organizations responsible for critical infrastructure services to manage cybersecurity risk.

NIST released a **Cybersecurity Framework**, as called for in Executive Order 13636, in February 2014. The Framework, developed to assist organizations in managing their cybersecurity risk, is technology neutral and relies on existing standards, guidance, and best practice to provide...

*a common language for describing current and target states of security, identifying and prioritizing changes needed, assessing progress and fostering communications with stakeholders. It is meant to complement, not replace, existing cybersecurity programs.*

The Framework is designed to provide a common taxonomy and mechanism for organizations to:

- Describe their current cybersecurity posture;
- 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.

### **Control System Cybersecurity Strategy and Roadmaps**

In 2004, Department of Homeland Security’s National Cybersecurity Division (NCSD) established the Control Systems Security Program (CSSP), which was chartered to work with control systems security stakeholders through awareness and outreach programs that encourage and support coordinated control systems security enhancement efforts. In 2008, the CSSP established the Industrial Control Systems Joint Working Group (ICSJWG) as a coordination body to facilitate the collaboration of control system stakeholders and to encourage the design, development and deployment of enhanced security for control systems.

Leveraging the efforts of individual sectors such as Energy, Water, and Chemical developing roadmaps to secure their industrial control systems, the DHS National Cybersecurity Division (NCSD), with volunteers from the Industrial Control Systems Joint Working Group (ICSJWG) and industry stakeholder organizations, developed a **Cross-Sector Roadmap to Secure Control Systems** to coordinate the efforts across multiple sectors and help develop programs and risk mitigation measures that align with the sector’s plan while maintaining a cross sector perspective. Issued in 2011, the Roadmap provided a plan for voluntarily improving cybersecurity across all critical infrastructure/key resources (CIKR’s) that employ industrial control systems.

Recognizing the widespread use of control systems in transportation and the economic and social impacts of a transportation cyber-event, the Department of Homeland Security (DHS)

also issued *The Transportation Industrial Control Systems (ICS) Cybersecurity Standards Strategy* in 2012. The DHS recommended standardizing transportation ICS cybersecurity practices because “control systems cybersecurity is a fledgling concern in the transportation sector, and preliminary research has illustrated that while some modes have developed relevant standards, most of them have failed to address ICS cybersecurity”. The DHS Standards Strategy summarized the state of cybersecurity by transportation mode, identified short and long-term goals to address gaps in ICS cybersecurity standards, and outlined the estimated cost, timeline, and deliverables associated with meeting those goals.

According to the DHS Standards Strategy summary of the transportation modes ICS standardization activities:

- Aviation has made great strides in securing CS for aircraft; however, cybersecurity standards have not addressed CS in airports. *Airworthiness Security Methods and Considerations and Airworthiness Security Process Specification* were published in 2010. Neither document is publicly available.
- Maritime currently has no standards to address control systems located in ports, terminals, and onboard vessels. The USCG Cyber Command (USCG-CC) recognized the need for sound cybersecurity policy, and created the Command, Control, Communication, Computers, and Information Technology (C4&IT) Strategic Plan.
- Transit is currently developing ICS cybersecurity standards through APTA. The freight rail industry does not have a corresponding cybersecurity standards effort. *APTA Recommended Practice, Securing Control and Communications Systems in Transit Environments, Part I: Elements, Organization and Risk Assessment/Management*, was published in July 2010. *Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones* was published in 2013. *Part 3a: Attack Modeling Security Analysis* was published in early 2015. *Part 3B: Protecting the Operationally Critical Security Zone* is anticipated at a later date.
- Because the highway mode was not actively developing control systems cybersecurity standards at the time of the DHS Standards Strategy publication, DHS has begun to engage standards development organizations (SDO's) and federal agencies to create a highway ICS working group. The focus of the group will be identifying and classifying common highway ICS systems as a start to create a highway ICS cybersecurity standard.
- Pipeline mode has developed ICS cybersecurity standards. *API Standard 1164: Pipeline SCADA Security* was published in 2009. *Control Systems Cybersecurity Guidelines for the Natural Gas Pipeline Industry* was published in 2011.

DHS and the Department of Transportation John A. Volpe National Transportation Systems Center (Volpe Center) issued *A Roadmap to Secure Control Systems in Transportation* in 2012. The document views cybersecurity and ICS as inseparable and integrated throughout the transportation sector. The major goals of the Roadmap are:

- to build a "culture of cybersecurity" that includes an ICS cybersecurity governance model and a cybersecurity awareness training program
- to assess and monitor risk that includes identifying risk management framework and standards, roles and responsibilities, and developing and implementing a risk management model and strategy

- to develop and implement risk reduction and mitigation measures such as securing interfaces between ICS and other systems and encouraging development of self-defending technologies built-in to the ICS infrastructure
- to manage incidents including research new effective detection and response tools. Near- term objectives focus on assessing risk, with long-term objectives focused on establishing continuous and automated risk monitoring programs and regularly measuring risk management performance.

### ***National and Regional Support Resources***

As part of these federal initiatives, a number of national and regional support programs have been established, summarized below.

#### *US Department of Transportation (USDOT) Cybersecurity Action Team*

The US Department of Transportation (USDOT) developed a Cybersecurity Action Team, as part of Executive Order 13636, to implement o the Department’s Cyber Incident Response Capability Program. The team monitors, alerts and advises the ITS and surface transportation communities of incidents and threats, and leverages the extensive body of assessments and research done by Federal Highway Administration (FHWA) staff related to the security threats and vulnerabilities of the United States’ transportation systems.

#### *US-CERT and Industrial Control Systems (ICS-CERT) Cyber Information Sharing and Collaboration Program*

The US Computer Emergency Readiness Team (US-CERT), part of DHS' National Cybersecurity and Communications Integration Center (NCCIC), provides technical assistance, coordinates cyber information sharing and proactively manage cyber risks through its 24x7 operations center. US-CERT distributes vulnerability and threat information through its National Cyber Awareness System (NCAS), and operates a Vulnerability Notes Database to provide technical descriptions of system vulnerabilities.

*Incident Hotline: 1-888-282-0870*

*Website: <https://www.us-cert.gov/>*

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) operates cybersecurity operations centers focused on control systems security as part of the National Cybersecurity and Communications Integration Center (NCCIC). The team:

- Responses to and analyses industrial control systems (ICS) related incidents
- Provides onsite support for incident response and forensics
- Conducts malware analysis
- Coordinates responsible disclosure of ICS vulnerabilities/mitigations
- Shares vulnerability information and threat analysis through information products and alerts
- Provides security awareness training courses (see <http://ics-cert.us-cert.gov/Training->

Available-Through-ICS-CERT).

<https://ics-cert.us-cert.gov/>

- Transportation Security Administration (TSA)

The TSA has authority to regulate cybersecurity in the transportation sector and provides cybersecurity pamphlets, a weekly newsletter, cybersecurity exercise support, and incident-specific threat briefings. TSA has pursued collaborative and voluntary approaches with industry. TSA DHS facilitates the Cybersecurity Assessment and Risk Management Approach (CARMA) for companies requesting assessments. TSA has hosted cybersecurity-focused Intermodal Security Training and Exercise Program (I-STEP) exercises, most recently in August 2014.

TSA and its industry partners established the Transportation Systems Sector Cybersecurity Working Group (TSSCWG) to advance cybersecurity across all transportation modes. The TSSCWG strategy, completed in mid-2012, stated,

*The sector will manage cybersecurity risk through maintaining and enhancing continuous awareness and promoting voluntary, collaborative, and sustainable community action.*

The TSSCWG is developing implementation guidance for adoption of the NIST Framework.

- Other Federal Departments and Agencies

National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is an agency of the U.S. Department of Commerce. The Computer Security Division (CSD), a component of NIST's Information Technology Laboratory (ITL), provides standards and technology to protect information systems against threats to information and services.

***Executive Order 13636, Improving Critical Infrastructure Cybersecurity (2013)*** directed NIST to work with stakeholders to develop a voluntary cybersecurity framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. <http://www.nist.gov/cyberframework/>

A ***Cybersecurity Framework (CSF) Reference Tool***, a runtime database solution, have been created the allows the user to browse the Framework Core by functions, categories, subcategories, informative references, search for specific words, and export the current viewed data to various file types.

[http://www.nist.gov/cyberframework/csf\\_reference\\_tool.cfm](http://www.nist.gov/cyberframework/csf_reference_tool.cfm)

National Institute of Standards and Emergency Technology (CERT®), Source on Insider Threat and Prevention <http://csrc.nist.gov/index.html>

## NIST National Vulnerability Database

National Vulnerability Database (NVD) is the U.S. government repository of standards-based vulnerability management data that includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.

<http://nvd.nist.gov>

NIST Computer Security Division's Computer Security Resource Center (CSRC) facilitates broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia. The CSRC is the primary gateway for gaining access to NIST computer security publications, standards, and guidelines plus other useful security-related information.

<http://csrc.nist.gov/publications/PubsSPs.html>

NIST has published over 300 Information Security guides that include Federal Information Processing Standards (FIPS), the Special Publication (SP) 800 series, Information Technology Laboratory (ITL) Bulletins, and NIST Interagency Reports (NIST IR). Most commonly referenced NIST publications include:

- ***Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook (1995)***. Elements of security, roles and responsibilities, common threats, security policy, and program management. Initially created for the federal government, most practices are applicable to the private sector.
- ***Special Publication 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems (1996)*** describes common security principles that are used. It provides a high level description of what should be incorporated within a computer security policy. It describes what can be done to improve existing security as well as how to develop a new security practice. Eight principles and fourteen practices are described within this document.
- ***Special Publication 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model (2014)***. Learning-continuum model, security literacy and basics, role-based training.
- ***Special Publication 800-30, Risk Management Guide for Information Technology Systems (2012)***. Risk management, assessment, mitigation.
- ***Special Publication 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems (2010)***
- ***Special Publication 800-39 Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View (2011)***.
- ***Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations (2013)***. Security control fundamentals, baselines by system-impact level, common controls, and tailoring guidelines that are applied to a system to make it "more secure".
- ***Special Publication 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, (2008)***. Security objectives and types of potential losses, assignment of impact levels and system security category.



- ***Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security (2014)***. Overview of industrial control systems (ICS), threats and vulnerabilities, risk factors, incident scenarios, security program development.
- ***Special Publication 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i (2007)***
- ***Special Publication 800-100, Information Security Handbook: A Guide for Managers (2006)***. Governance, awareness and training, capital planning, interconnecting systems, performance measures, security planning, contingency planning.
- ***Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (2010)***. Identifying, PII, impact levels, confidentiality safeguards, incident response.

Recent draft publications include:

- ***Special Publication 800-150 Guide to Cyber Threat Information Sharing, Draft (2014)***.
- ***Special Publication 800-160 Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems, Draft (2014)***.

*Information Sharing and Analysis Centers (ISAC's)*

<http://www.isaccouncil.org/home.html>

The purpose of ISAC is to serve as the conduit for cross-modal lessons learned and best practices in ICS cybersecurity, and to provide a forum for partnership, outreach, and information sharing.

- Surface Transportation Information and Sharing Analysis Center

<https://www.surfacetransportationisac.org/>

The ST-ISAC was formed at the request of the Department of Transportation. The ISAC provides a secure cyber and physical security capability for owners, operators and users of critical infrastructure. Security and threat information is collected from worldwide resources, then analyzed and distributed to members to help protect their vital systems from attack. The ISAC also provides a vehicle for the anonymous or attributable sharing of incident, threat and vulnerability data among the members. Members have access to information and analytical reporting provided by other sources, such as the U.S. and foreign governments; law enforcement agencies, technology providers and international computer emergency response teams (CERT's).

- Public Transportation Information Sharing and Analysis Center

<http://www.apta.com/resources/safetyandsecurity/Pages/ISAC.aspx>

The PT-ISAC is a trusted, sector-specific entity which provides to its constituency a 24/7 Security Operating Capability that established the sector's specific information/intelligence requirements for incidences, threats and vulnerabilities. Based on its sector-focused subject matter analytical expertise, the ISAC then collects, analyzes, and disseminates alerts and incident reports It provides to its membership and helps the government understand impacts for their sector. It provides an electronic, trusted

ability for the membership to exchange and share information on all threats, physical and cyber, in order to defend public transportation systems and critical infrastructure. This includes analytical support to the Government and other ISAC's regarding technical sector details and in mutual information sharing and assistance during actual or potential sector disruptions, whether caused by intentional or natural events.

- Over the Road Bus Information Sharing and Analysis Center (OTRB ISAC)

The OTRB ISAC provides cyber and physical security warning and incident reporting for the OTR transportation segment. Information and news are compiled and extracted from multiple sources by OTRB-ISAC analysts for the purpose of supporting ISAC member homeland security awareness. News alerts and reports are distributed to members by the Over the Road Bus – Information Sharing & Analysis Center (OTRB-ISAC).

- MultiState-ISAC (MS-ISAC)

<http://msisac.cisecurity.org/>

The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. The MS-ISAC 24x7 cybersecurity operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a collaborative state and local government-focused cybersecurity entity that is significantly enhancing cyber threat prevention, protection, and response and recovery throughout the states of our nation. The mission of the MS-ISAC is to provide a common mechanism for raising the level of cybersecurity readiness and response in each state/territory and with local governments. The MS-ISAC provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between and among the states, territories and with local government.

- Supply Chain ISAC

<https://secure.sc-investigate.net/SC-ISAC/ISACHome.aspx>

The Supply Chain ISAC offers the most comprehensive forum for collaboration on critical security threats, incidents and vulnerabilities to the global supply chain. Its mission is to facilitate communication among supply chain dependent industry stakeholders, foster a partnership between the private and public sectors to share critical information, collect, analyze and disseminate actionable intelligence to help secure the global supply chain, provide an international perspective through private sector subject matter experts and help protect the critical infrastructure of the United States.

### *National Cyber Investigative Joint Task Force – Analytical Group*

In 2008, the U.S. President mandated the National Cyber Investigative Joint Task Force (NCIJTF) to be the focal point for all government agencies to coordinate, integrate, and share information related to all domestic cyber threat investigations. The FBI is responsible for developing and supporting the joint task force, which includes 19 intelligence agencies and law enforcement.

<http://www.fbi.gov/about-us/investigate/cyber/ncijtf>

*Internet Crime Complaint Center (IC3)*

The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). Internet crime complaints are reported online on the IC3 site. IC3 analysts review and research the complaints, disseminating information to the appropriate federal, state, local, or international law enforcement or regulatory agencies for criminal, civil, or administrative action, as appropriate. <http://www.ic3.gov/default.aspx>

*InfraGard*

InfraGard is a partnership between the FBI, state and local law enforcement agencies, and the private sector - businesses, academic institutions and other participants - dedicated to sharing information and intelligence to prevent hostile acts against the U.S. With over 80 chapters, InfraGard chapters conduct local meetings pertinent to their area. <https://www.infragard.org/>

*National Cybersecurity Center of Excellence (NCCoE)*

Established in 2012 through a partnership among NIST, the State of Maryland and Montgomery County, the National Cybersecurity Center of Excellence is dedicated to furthering innovation through the rapid identification, integration and adoption of practical, standards-based cybersecurity solutions. <http://nccoe.nist.gov/>

## **Appendices**

Appendix A References and Sources

Appendix B Acronyms

Appendix C Glossary

# References and Sources

## Contents

<a href="#">General Cybersecurity</a> .....	1
<a href="#">Cybersecurity and Transportation</a> .....	2
<a href="#">Industrial Control Systems Cybersecurity</a> .....	4
<a href="#">Transportation System Vulnerabilities</a> .....	6
<a href="#">Risk Assessment and Management</a> .....	9
<a href="#">Countermeasures</a> .....	10
<a href="#">Training</a> .....	13
<a href="#">Standards and Recommended Practices</a> .....	14

## **General Cybersecurity**

Cyber Attacks, E. Amoroso, Elsevier, 2010

“Key Principles of Cyber Security”, Accenture, 2013

Enterprise Information Security and Privacy, J. L. Bayuk, D. Schutzer, Artech House, January 2009

Cyber Security Policy Guidebook, Bayuk, J., J. Healy, et al. , Hoboken, NJ, Wiley, 2012

Engineering Information Security, S. Jacobs, Wiley, 2011

Cybercrime, Cyberpower and National Security, F. D. Kramer, S. H. Starr and L. Wentz, eds., Potomac Books, Inc., 2009

CIP Report: Cybersecurity, George Mason University Center for Infrastructure Protection  
Volume 10, Number 10, April 2012

The IT Industry’s Cybersecurity Principles for Industry and Government, Information  
Technology Industry Council, 2011

Glossary of Key Information Security Terms, National Institute of Standards and Technology  
(NIST), NISTIR 7298, Revision 2, May 2013

Special Publication (SP) 800-100 : Information Security Handbook: A Guide for Managers,  
NIST, March 2007

Minimum Security Requirements for Federal Information and Information Systems, Federal Information Processing Standards (FIPS) Publication 200, March 2006

“Thirteen Principles to Ensure Enterprise System Security”, G. McGraw, SearchSecurity, 2013

“Least Privilege and More”, F. B. Schneidier. Cornell University, IEEE Computer Society, 2003

"The Protection of Information in Computer Systems", J. Saltzer, M. D. Schroeder, Proceedings of the IEEE 63, 9 pp.1278-1308, 1975

### **Cybersecurity Surveys**

Department Of Commerce Computer Security Survey, 2001

Rand National Computer System Security Survey, 2005

InformationWeek 2012 Federal Cybersecurity Survey, March 2012

2012 Deloitte-NASCIO Cybersecurity Study "State governments at risk: a call for collaboration and compliance", 2012

Global State of Information Security Survey, Price Waterhouse Cooper, 2013

ICS SCADA Cyber Security Survey, SANS 2013

Firefly, 2014

### ***Cybersecurity and Transportation***

ABI Research, Cellular M2M Connections Will Show Steady Growth to Top 297 Million in 2015 October 18, 2010

American Public Transportation Association, Recommended Practice: Securing Control and Communications Systems in Rail Transit Environment, Part 1: Elements, Organization and Risk Assessment/Management ; Part 2: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones; Part 3, 2010 -2015

American Public Transportation Association, Cybersecurity Considerations for Public Transportation, 2014

American Public Transportation Association, Recommended Practice on Selecting Cameras, Recording Systems, High-Speed Networks and Trainlines for CCTV Systems, 2011

API Standard 1164: Pipeline SCADA Security, 2009

System Assurance, Operations and Reactive Defense for Next Generation Vehicles, Intelligent Highway Infrastructure, and Road User Services, S. H. Bayless, S. Murphy, A. Shaw, ITS Technology Scan Series, January 2014

“Railway Security Issues: A Survey Of Developing Railway Technology”, A. H. Carlson, D. Frincke and M. J. Laude, Proceedings of the International Conference Computing, Communications, and Control Technology (CCCT), 2003

"Railroads and the Cyber Terror Threat", A. Carlson, D. Frincke, and M. Laude Technical Report CSDS-DF-TR-03- 14, Center for Secure and Dependable Systems, University of Idaho, 2003

The Roadmap to Secure Control Systems in Transportation, DHS 2012

Assessing the Security and Survivability of Transportation Control Networks, P. Oman, National Institute for Advanced Transportation Technology, 2005

Introduction to Cyber Security Issues for Transportation, T3 Webinar, M. G. Dinning, Volpe and RITA, US DOT, December 2011

Cyber Concerns for Transportation Organizations – an Overview, FHWA Resource Center in San Francisco Office of Technical Service - Operations Technical Service Team, E. Fok Webinar, RITA, US DOT, December 2011

Cyber Security Challenges: Protecting Your Transportation Management Center, Fok, Edward, ITE Journal, February, 2015.

“Transportation Security”, Hunt, S. in Enterprise Information Security and Privacy , C. W. Axelrod, J. Bayuk and D. Schutzer eds., Artech House: 181-189, 2009

ITSA Connected Vehicle Assessment – Cybersecurity and Dependable Transportation, Connected Vehicle Technology Scan Series, 2012-2014

ITSA Machine to Machine Communications, Connected Vehicle Technology Scan Series, 2011-2012 ITSA Website, [www.itsa.gov](http://www.itsa.gov)

Cybersecurity Best Practices, National Highway and Traffic Safety Agency (NHTSA), 2014

Industrial Control Systems, the NIST Risk Management Framework, and Special Publication 800-82, NIST, Nov 2012 PPT

NIST Special Publication 800-82, Guide to Industrial Control Systems Security, Revision 4, 2015

TCRP 80 Transit Security Update: A Synthesis of Transit Practice, Y. Nakanishi, Transportation Research Board, 2009

Assessing the Security and Survivability of Transportation Control Networks, P. Oman, National Institute for Advanced Transportation Technology, 2005

Connected Vehicle Research Program Presentation, Sheehan, Robert, ITSJPO, USDOT

Transportation Research Board Special Report 274: Cybersecurity of Freight Information Systems: A Scoping Study, Transportation Research Board, 2003

“The Roadmap to Secure Control Systems in Transportation”, National Transportation Systems Center VOLPE, Presentation made at TRB Cyber Subcommittee Teleconference, October 2012

Cyber-Physical Systems. <http://cyberphysicalsystems.org/> accessed March 6, 2015

SECUR-ED Cyber-security roadmap for PTOs

“Cybersecurity and Dependable Transportation”, Outreach Presentation, TSA Cyber Security Working Group Cyber Security Awareness and Outreach, Information Assurance and Cyber Security Division (IAD), Office of Information Technology (OIT), TSA/DHS, 2012

USA PATRIOT Act of 2001, P.L.107-56

Executive Order 13636 (EO), “Improving Critical Infrastructure Cybersecurity”, February 12, 2013

National ITS Architecture 7.1, U.S. Department of Transportation ITS Joint Program Office

FHWA Presentation Slides on Cyber Security TRB: Connected Vehicles Security, Van Duren, Drew, Oct., 2014

A Summary of Cybersecurity Best Practices, Volpe, NHTSA, October, 2014

## ***Industrial Control Systems Cybersecurity***

American Public Transportation Association, Recommended Practice: Securing Control and Communications Systems in Rail Transit Environment, Part 1: Elements, Organization and Risk Assessment/Management, July 2010. Part 2: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones

Hidden Vulnerabilities in SCADA and Critical Infrastructure Systems, E. Byres, 2008

Critical Infrastructure Protection: Challenges In Securing Control Systems, R. Dacey, Government Accountability Office (GAO), 2003

Transportation Industrial Control Systems Cybersecurity Standards Strategy, DHS, 2012



Security for Critical Infrastructure SCADA Systems, A. Hildick-Smith, SANS Institute, 2005

“Understanding the Physical and Economic Consequences of Attacks Against Control Systems”, Y.Huang, A. A. Cárdenas, S. Amin, Z.Lin, H.Tsai, S. Sastry, International Journal of Critical Infrastructure Protection Vol 2, Issue 2, October 2009

Lessons Learned from Cybersecurity Assessments of SCADA Systems, National SCADA TestBed Program, Idaho National Laboratory, 2006

A Baseline Standard for Industrial Control Systems, ISA/IEC-62443

Cybersecurity for Industrial Control Systems, Macaulay, Tyson and Singer, Bryan,. CRC Press, 2012

Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, Special Publication 800-82, NIST, September 2006

NIST Special Publication 800-82, Guide to Industrial Control Systems Security, 2011

“Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems”, P. Oman, E.O. Schweitzer III, D. Frincke, Paper #4, 27th Annual Western Protective Relay Conference, Spokane, WA, 2000

“SCADA HoneyNet Project: Building Honeypots for Industrial Networks”, V. Pothamsetty and M. Franz, SourceForge, 2008

“Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies”, Rinaldi, et al., IEEE Control Systems Magazine, 2001

“Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems”, R. J. Robles, M. Choi, International Journal of Grid and Distributed Computing Vol.2, No.2, June 2009

“SCADA System Vulnerabilities to Field-Based Cyber Attacks”, W. T. Shaw, Electric Energy, September-October, 2004

“Common Vulnerabilities in Critical Infrastructure Control Systems”, Stamp, Dillinger, Young, DePoy, Sandia National Laboratories, May 2003

“Vulnerabilities in SCADA and Critical Infrastructure Systems”, R. J. Robles, M. Choi, E. Cho, S. Kim, G. Park, S. Yeo, International Journal of Future Generation Communication and Networking, Vol. 1, No. 1, 2008

Control System Devices: Architectures and Supply Channels Overview, Schwartz, M. D., J. Mulder, et al, Albuquerque, New Mexico, Sandia National Laboratories, 2010

“Cyberthreats, Vulnerabilities and Attacks on SCADA”, R. Tang, UC Berkeley, 2009

“Protecting Critical Infrastructure: SCADA Network Security Monitoring”, Tenable Network security whitepaper, August 1, 2008

Industrial Network Security, 2nd Edition, Teumim, David J., International Society of Automation, 2010

Protecting Industrial Control Systems from Electronic Threats, Weiss, J., Momentum Press, 2010

## ***Transportation System Vulnerabilities***

American Public Transportation Association, Recommended Practice: Securing Control and Communications Systems in Rail Transit Environment, Part 1: Elements, Organization and Risk Assessment/Management, July 2010. Part 2:

Hidden Vulnerabilities in SCADA and Critical Infrastructure Systems, E. Byres, 2008

“Security Incidents and Trends in SCADA and Process Industries”, E. Byers, D. Leversage, M. Kube, The Industrial Ethernet Book, Issue 45, 2008

“Research Challenges for the Security of Control Systems”, A. A. Cárdenas, S. Amin, S. Sastry, 3rd USENIX workshop on Hot Topics in Security (HotSec '08). Associated with the 17th USENIX Security Symposium, San Jose, CA, USA. July 2008

Computer Emergency Response Team (CERT) <http://www.cert.org/>

Critical Infrastructure Protection: Challenges In Securing Control Systems, R. Dacey, Government Accountability Office (GAO), 2003

Resilient Military Systems and the Advanced Cyber Threat, Defense Science Board, 2013

Common Cybersecurity Vulnerabilities in Industrial Control Systems, U.S. Department of Homeland Security (DHS) National Cyber Security Division's Control Systems Security Program, May 2011

Introduction to Cyber Security Issues for Transportation, T3 Webinar, Michael G. Dinning, Volpe and RITA, US DOT, December 7, 2011

Cyber Concerns for Transportation Organizations – an Overview, FHWA Resource Center in San Francisco Office of Technical Service - Operations Technical Service Team, Edward Fok Webinar, RITA, US DOT, December 7, 2011

Cybersecurity Challenges: Protecting Your Transportation Management Centers, Edward Fok, ITE Journal, Feb. 2015

HP Tippingpoint Hactivist Survival Guide: Simplifying the Complex, Hewlett-Packard, 2013

Security for Critical Infrastructure SCADA Systems, A. Hildick-Smith, SANS Institute, 2005

“Understanding the Physical and Economic Consequences of Attacks Against Control Systems”, Y.Huang, A. A. Cárdenas, S. Amin, Z.Lin, H.Tsai, S. Sastry, International Journal of Critical Infrastructure Protection Vol 2, Issue 2, October 2009

Lessons Learned from Cybersecurity Assessments of SCADA Systems, National SCADA TestBed Program, Idaho National Laboratory, 2006

A Baseline Standard for Industrial Control Systems, ISA/IEC-62443

Cybersecurity for Industrial Control Systems, Macaulay, Tyson and Singer, Bryan,. CRC Press, 2012

National Institute of Standards and Emergency Technology (CERT), Source on Insider Threat and Prevention <http://csrc.nist.gov/index.html>

Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security, Special Publication 800-82, NIST, September 2006

NIST National Vulnerability Database <http://nvd.nist.gov>

NIST Special Publication 800-82, Guide to Industrial Control Systems Security, Revision 4, 2015

“Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems”, P. Oman, E.O. Schweitzer III, D. Frincke, Paper #4, 27th Annual Western Protective Relay Conference, Spokane, WA, 2000

Top 10 -2013: The Ten Most Critical Web Application Security Risks, Open Web Application Security Project (OWASP), 2013

“SCADA HoneyNet Project: Building Honeypots for Industrial Networks”, V. Pothamsetty and M. Franz, SourceForge, 2008

“Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies”, Rinaldi, et al., IEEE Control Systems Magazine, 2001

“Vulnerabilities in SCADA and Critical Infrastructure Systems”, R. J. Robles, M. Choi, E. Cho, S. Kim, G. Park, S. Yeo, International Journal of Future Generation Communication and Networking, Vol. 1, No. 1, 2008

“SCADA System Vulnerabilities to Field-Based Cyber Attacks”, W. T. Shaw, Electric Energy, September-October, 2004

“Common Vulnerabilities in Critical Infrastructure Control Systems”, Stamp, Dillinger, Young, DePoy, Sandia National Laboratories, May 2003

“Assessment of the Vulnerabilities of SCADA, Control Systems and Critical Infrastructure Systems”, R. J. Robles, M. Choi, International Journal of Grid and Distributed Computing Vol.2, No.2, June 2009

Control System Devices: Architectures and Supply Channels Overview, Schwartz, M. D., J. Mulder, et al, Albuquerque, New Mexico, Sandia National Laboratories, 2010

“Cyberthreats, Vulnerabilities and Attacks on SCADA”, R. Tang, UC Berkeley, 2009

“Protecting Critical Infrastructure: SCADA Network Security Monitoring”, Tenable Network security whitepaper, August 1, 2008

Industrial Network Security, 2nd Edition, Teumim, David J., International Society of Automation, 2010

“GPS Vulnerabilities”, K. Van Dyke, Presentation to the TRB Cyber Security Subcommittee, 2012

Protecting Industrial Control Systems from Electronic Threats, Weiss, J., Momentum Press, 2010

### **Vulnerability Databases and Threat Reports**

Source on Insider Threat and Prevention, National Institute of Standards and Emergency Technology, CERT  
<http://csrc.nist.gov/index.html>

NIST National Vulnerability Database  
<http://nvd.nist.gov>

Computer Emergency Response Team (CERT)  
<http://www.cert.org/>

Internet Storm Center  
<http://isc.sans.org/>

Fraudwatch International  
<http://fraudwatchinternational.com>  
CISCO 2014 Annual Security Report

Mandiant Threat Report 2014

Ponemon Institute Report 2014

Symantec Internet Security Threat Report: 2011, 2012 Trends

Verizon 2012 and 2013 Data Breach Investigations Reports

UK 2013 Information Security Breaches Survey, Price Waterhouse, 2013

## ***Risk Assessment and Management***

Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program, ANSI/ISA-62443-2-1 (99.02.01), 2009

American Public Transportation Association, Cybersecurity Considerations for Public Transportation, 2014

American Public Transportation Association, Recommended Practice: Securing Control and Communications Systems in Rail Transit Environment, Part 1: Elements, Organization and Risk Assessment/Management, July 2010.

Enterprise Security for the Executive: Setting the Tone at the Top, Bayuk, Jennifer, Praeger, 2010

Cyber Security Policy Guidebook, Bayuk, J., J. Healy, et al. Wiley, Hoboken, NJ, 2012

Convergence of Enterprise Security Organizations, Booz Allen Hamilton, 2005

Cybersecurity Challenges: Protecting Your Transportation Management Centers, Edward Fok, ITE Journal, Feb. 2015

NCHRP Report 525 Vol. 14. Security 101: A Physical Security Primer for Transportation Agencies, Frazier, E. et. al. Transportation Research Board, 2009

Developing an ICS Cybersecurity Incident Response Plan, ICS-CERT

Cybersecurity Evaluation Tool (CSET®), ICS-CERT

Risk Management/CEO Recommended Practices, DHS US- CERT

CEO Questions to Ask and Key Questions the Board Should Ask, DHS US-CERT

Annual Survey, International Risk Management Institute

COBIT 5 for Risk, Information System Audit and Control Association

NERC CIP-002-3 Critical Cyber Asset Identification

NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers

NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems, Revision 1, 2012

NIST Special Publication 800-39 Managing Information Security Risk

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, 2014

Guide to Developing a Cyber Security and Risk Mitigation Plan, National Rural Electric Cooperative Association, 2011

Leveraging Behavioral Science to Mitigate Cyber Security Risk, Shari Lawrence Pfleeger and Deanna D. Caputo, MITRE, 2012

Developing a Security-Awareness Culture –Improving Security Decision Making, SANS Institute, 2005

Control Systems Security Program, Sawin, D., Volpe Program Manager , Powerpoint Presentation given at DHS CSSP ICSJWG Conference, Seattle, Oct. 27, 2010

Electricity Subsector Cybersecurity Risk Management Process, U.S. Department of Energy, May 2012

Energy Sector Cybersecurity Framework Implementation Guidance, U.S. Department of Energy, 2015

## ***Countermeasures***

NIST information Security Guides: There are over 300 NIST information security publications that includes Federal Information Processing Standards (FIPS), the Special Publication (SP) 800 series, Information Technology Laboratory (ITL) Bulletins, and NIST Interagency Reports (NIST IR). Most commonly referenced NIST publications include:

Special Publication 800-12 An Introduction to Computer Security: The NIST Handbook is an overview of computer security and control areas that emphasizes the importance of the security controls and ways to implement them. Initially created for the federal government, most practices are applicable to the private sector.

Special Publication 800-14 describes common security principles that are used. It provides a high level description of what should be incorporated within a computer security policy. It describes

what can be done to improve existing security as well as how to develop a new security practice. Eight principles and fourteen practices are described within this document.

Special Publication 800-26 provides advice on how to manage IT security. This document emphasizes the importance of self-assessments as well as risk assessments.

Special Publication 800-30 Risk Management Guide for Information Technology Systems

Special Publication 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems

Special Publication 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations addresses the security controls that are applied to a system to make it "more secure".

Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security

Other NIST publications, listed by technical topics, include:

**Authentication, Authorization, and Access Control For Direct and Remote Connectivity**

NIST SP: 800-73-2, Interfaces for Personal Identity Verification (4 parts), September 2008.

NIST SP 800-76-1, Biometric Data Specification for Personal Identity Verification, 2007.

NIST SP: 800-57 Recommendation for Key Management, March 2007, Part 1, General (Revised); Part 2, Best Practices; Part 3, Application Specific Key Management Guidance (Draft), October 2008

NIST SP 800-82 Rev 1, Guide to Industrial Control Systems (ICS) Security, May 13, 2013.

Mix, S., Supervisory Control and Data Acquisition (SCADA) Systems Security Guide, EPRI, 2003.

Baker, Elaine, et al, NIST SP: 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007.

**Patch, Password, and Configuration Management**

NIST SP: 800-118, Guide to Enterprise Password Management (Draft)

NIST SP: 800-12, An Introduction to Computer Security: The NIST Handbook.

NIST SP: 800-40, Creating a Patch and Vulnerability Management Program, 2005.

Mix, S., Supervisory Control and Data Acquisition (SCADA) Systems Security Guide, EPRI, 2003.

Dzung, D., Naedele, M., Von Hoff, T., and Crevatin, M. "Security for Industrial Communication Systems," Proceedings of the IEEE. Institute of Electrical and Electronics Engineers Inc. 2005.

NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, 2015.

NIST SP 800-53 Rev 4, Recommended Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

Cyber Attacks, E. Amoroso, Elsevier, 2010

Enterprise Information Security and Privacy, J. L. Bayuk, D. Schutzer, Artech House, January 2009

Critical Controls for Effective Cyber Defense, 20 Critical Security Controls - Version 4.1, COBIT, 2013

Critical Controls for Effective Cyber Defense, 20 Critical Security Controls - Version 4.1, Council on Cybersecurity, March 2013

Cybersecurity Challenges: Protecting Your Transportation Management Centers, Edward Fok, ITE Journal, Feb. 2015

ICS Cybersecurity Response to Physical Breaches of Unmanned Critical Infrastructure Sites, SANS Analyst Whitepaper, ICS CERT, 2014

Cybersecurity Best Practices, National Highway and Traffic Safety Agency (NHTSA), 2014

NCHRP Report 525 Vol. 14. Security 101: A Physical Security Primer for Transportation Agencies, Frazier, E. et. al. Transportation Research Board, 2009

21 Steps to Improve Cyber Security of SCADA Networks, U.S. Department of Energy, Infrastructure Security and Energy Restoration Committee, 2007

Cybersecurity Procurement Language for Control Systems, U.S. Department of Homeland Security and U.S. Department of Energy, 2009

Cybersecurity Procurement Language of Energy Delivery System, Energy Sector Cybersecurity Working Group, 2014

Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies, U.S. Department of Homeland Security, October 2009

## **BYOD**

Bring Your Own Device: A Toolkit to Support Federal Agencies Implementing Bring Your Own Device, Digital Services Advisory Group and Federal Chief Information Officers Council, August 23, 2012

## **General IT Security Resources**

Federal Desktop Core Configuration <http://fdcc.nist.gov>

Microsoft Technet <http://technet.microsoft.com>

ISO/IEC 27000 Book: "Standard of Good Practice"

## **Wireless Assets**

NIST SP800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i



## ***Training***

Recommended Practice on Security Awareness Training for Transit Employees, APTA, 2012

A Role-Based Model for Federal Information Technology/Cybersecurity Training, NIST SP 800-16, Revision 1 (Third Draft) October, 2014

Building an Information Technology Security Awareness and Training Program, NIST SP800-50, October, 2003

2014 Cybersecurity Framework, Version 1.0, NIST, 2014

Information Security Training Requirements: A Role- and Performance-Based Model, NIST SP800-16 Revision 1, 1998

National Rural Electric Cooperative Association, Guide to Developing a Cybersecurity and Risk Mitigation Plan, 2011

NCHRP Report 685 Strategies to Attract and Retain a Capable Transportation Workforce, Transportation Research Board, 2011

NCHRP Report 693 Attracting, Recruiting and Retaining a Skilled Staff for Transportation Systems Operations and Management, Transportation Research Board, 2012

TCRP Report 162 Building a Sustainable Workforce in the Public Transportation Industry – A Systems Approach, Transportation Research Board, 2013

NCHRP Report 793, Incorporating Transportation Security Awareness into Routine State DOT Operations and Training , Transportation Research Board, 2014

NCHRP Synthesis Report 468 on Interactive Training for All-Hazards Emergency Planning, Preparation, and Response for Maintenance & Operations Field Personnel, Transportation Research Board, 2015

Transportation Roadmap, DHS, August, 2012

NIST SP 800-16 (1998) provides the IT security learning continuum model including 26 roles and role-based matrices and 46 training matrix cells, terms and concepts for IT security literacy, training content categories, and functional specialties.

NIST SP 800-50 Building an Information Technology Security Awareness and Training Program (2003) describes the life cycle of a cybersecurity awareness and training program. The life cycle includes needs assessment and an implementation strategy,

NIST SP 800-16 Appendices contain helpful information on function areas, knowledge and skills, and roles. Appendix A provides information on Function Areas including a general description of the area and the Learning Objectives for each function. Appendix B contains the

Knowledge and Skills Catalog and Appendix C presents the roles matrix using generic roles and titles.

## ***Standards and Recommended Practices***

### **NIST**

The National Institutes of Standards and Technology (NIST) has the responsibility, along with the private sector, to develop a framework of baseline standards for cybersecurity of the nation's critical infrastructure, derived from the Presidential Directive on Cyber Security. The NIST framework relies on existing standards, guidance, and best practices, drawing heavily from guidance developed by NIST for the Federal Information Security Management Act. Selected examples of the NIST/FIPS publications include:

Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information System (March 2006)

National Institute of Standards and Technology Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995. Elements of security, roles and responsibilities, common threats, security policy, program management.  
<http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>.

National Institute of Standards and Technology Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998. Learning-continuum model, security literacy and basics, role-based training.  
<http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf>.

National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems, July 2002. Risk management, assessment, mitigation. <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.

National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations, August 2009. Security control fundamentals, baselines by system-impact level, common controls, tailoring guidelines, catalog of controls in 18 families. <http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf>.

National Institute of Standards and Technology Special Publication 800-60, Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008. Security objectives and types of potential losses, assignment of impact levels and system security category. [http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60\\_Vol1-Rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf).

National Institute of Standards and Technology Special Publication 800-82 (Final Public Draft), Guide to Industrial Control Systems (ICS) Security, September 2008. Overview of industrial

control systems (ICS), threats and vulnerabilities, risk factors, incident scenarios, security program development. [http://csrc.nist.gov/publications/drafts/800-82/draft\\_sp800-82-fpd.pdf](http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf).

National Institute of Standards and Technology Special Publication 800-100, Information Security Handbook: A Guide for Managers, October 2006. Governance, awareness and training, capital planning, interconnecting systems, performance measures, security planning, contingency planning. <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>.

National Institute of Standards and Technology Special Publication 800-122 (Draft), Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), January 2009. Identifying, PII, impact levels, confidentiality safeguards, incident response. <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>.

National Institute of Standards and Technology Special Publication 800-39(Final Public Draft), Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View, December 2010. <http://csrc.nist.gov/publications/drafts/800-39/draft-SP800-39-FPD.pdf>. The ***Roadmap to Secure Control Systems in the Transportation Sector*** (Transportation Roadmap), which describes a plan for voluntarily improving industrial control systems (ICSs) cybersecurity across all transportation modes: aviation, highway, maritime, pipeline, and surface transportation, summarized the currently existing cybersecurity standards for the various transportation modes.

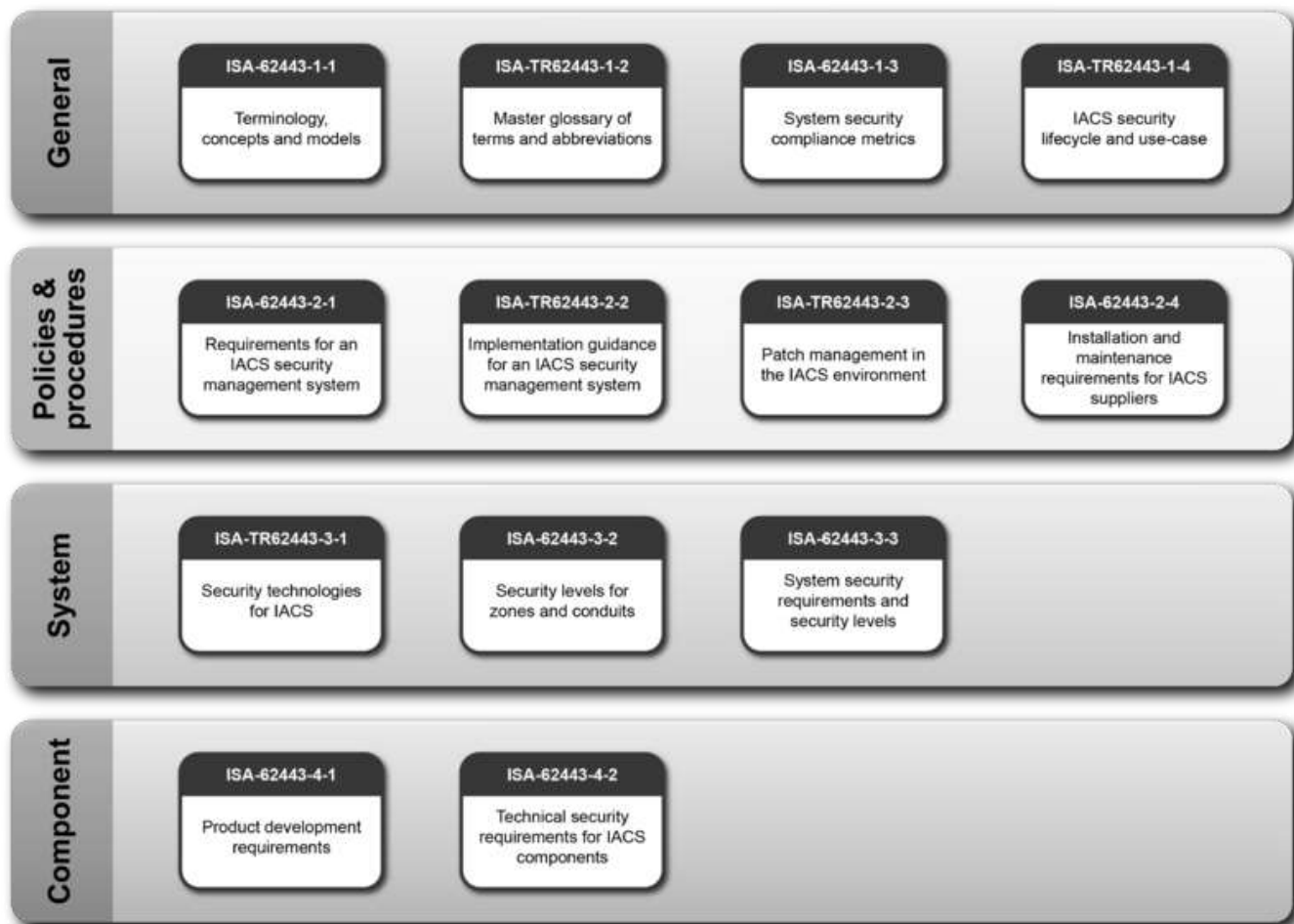
## ISO and ISA

The International Organization for Standardization (ISO), the Information Systems Audit (ISA) and the Control Association (ISACA) Control Objectives for Information and related Technology (COBIT) have developed standards that provide the industry with best practices.

ISO/IEC have developed a series of standards “use by those responsible for initiating, implementing or maintaining information security management systems.”

- ISO/IEC 27001: Information Security Management
- ISO/IEC 27002: Information Technology. Security techniques. Code of practice for information security management
- ISO/IEC 27035: Security Incident Management
- ISO/IEC 27017 [Not yet released]: Cloud Security
- ISO/IEC 22301: Business Continuity Management, published in May 2012, is the international standard for business continuity management

ISA/IEC-62443 (formerly ISA-99) is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS). These documents were originally referred to as ANSI/ISA-99 or ISA99 standards, as they were created by the International Society for Automation (ISA) and publicly released as American National Standards Institute (ANSI) documents. In 2010, they were renumbered to be the ANSI/ISA-62443 series. The chart below provides an overview of the relevant ISA/IEC- 62443 standards.



## NERC CIP

North American Electric Reliability Council (NERC), have developed Critical Infrastructure Protection (CIP) Standards available at <http://www.nerc.com/page.php?cid=2|20>:

- CIP-002-3, Critical Cyber Asset Identification
- CIP-003-3, Security Management Controls
- CIP-004-3, Personnel and Training
- CIP-005-3, Electronic Security Perimeter(s)
- CIP-006-3, Physical Security of Critical Cyber Assets
- CIP-007-3, Systems Security Management
- CIP-008-3, Incident Reporting and Response Handling
- CIP-009-3, Recovery Plans for Critical Cyber Assets
- “Security Guidelines for the Electricity Sector: Vulnerability and Risk Assessment,” 1.0. <http://www.esisac.com/publicdocs/Guides/V1-VulnerabilityAssessment.pdf>

The CIP standards are also included in the collected Reliability Standards for the Bulk Electric Systems of North America, June 2010, [http://www.nerc.com/files/Reliability\\_Standards\\_Complete\\_Set.pdf](http://www.nerc.com/files/Reliability_Standards_Complete_Set.pdf).

## US CERT

A more in-depth description of typical ICSs and their vulnerabilities and currently available general security enhancements can be found on the United States Computer Emergency Readiness Team (USCERT) Control System website at the following URL: [http://www.uscert.gov/control\\_systems/csvuls.html](http://www.uscert.gov/control_systems/csvuls.html), and in the National Institute of Standards and Technology (NIST) Special Publication 800-82, “Guide to Industrial Control Systems (ICS) Security, Recommendations of the National Institute of Standards and Technology.”

## APTA

APTA’s cybersecurity initiatives focus on transit systems and are carried out through the following Working Groups:

- The Enterprise Cybersecurity Working Group
- The Control & Communications Security Working Group (CCSWG)

APTA (through the CCSWG) has produced two of three Recommended Practices on Securing Control and Communications Systems in Rail Transit Environments. The CCSWG uses standards from the North American Electric Reliability Corporation Critical Infrastructure Protection program (NERC-CIP), NIST, ISA, and the IEEE to develop these Recommended Practices which are as follows:

- Part 1 - Elements, Organization, and Risk Assessment/Management was released in July, 2010. Part I focuses on the importance of control and communications security to a transit agency, describes systems that comprise a typical transit control and communication systems, identifies the steps required for a successful program, and introduces risk assessment.
- Part 2 - Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones was released in June, 2013. This Part describes “Defense-in-Depth” for rail communications and control systems security, defines security zone classifications, and a minimum set of security controls for the most critical zones, the safety-critical security zone (SCSZ) and the fire, life-safety security zone (FLSZ). The recommendations apply to new rail projects or major upgrades, not the retrofitting of legacy systems.
- Part 3 will continue to address security zones and introduce attack modelling for rail transit.
  - Subpart 3a will present the APTA Attack Modeling Security Analysis for Transit Agencies and their Systems Integrators and Vendors. The Attack Tree Analysis Scope, Attack Modeling Process, and a Case Study of the Process will be included. The expected publication date of this Subpart is January, 2015.
  - Subpart 3b will cover the Operationally Critical Security Zone (OCSZ), in the same manner as how Part 2 addressed the Safety Critical Security Zone (SCSZ) and the Fire, Life Safety Security Zone (FLSZ); the development of this Subpart will occur in 2015.
  - Subpart 3c will address the application of the three security zones to rail transit vehicles.

## Wireless Communications

Wireless communications and wireless security standards include the following:

- IEEE 802.15.4 building automation and control systems
- IEEE 802.11 WLAN or Wi-Fi
- IEEE 802.16 WiMax for long-distance broadband
- Bluetooth, proprietary 900 MHz or 2.4 GHz (license-free spread spectrum), fixed-frequency radios (100 to 800 MHz, typically licensed), and cellular GSM/GPRS-based communications.
- IEEE 1474.3-2008 IEEE Recommended Practice for Communications-Based Train Control (CBTC) System Design and Functional Allocations

# Acronyms

NIST Interagency Report 7581 System And Network Security Acronyms and Abbreviations, September 2009, contains a list of acronyms and abbreviations with their generally accepted or preferred definitions.

<b>ACL</b>	Access Control List
<b>ARP</b>	Address Resolution Protocol
<b>AASHTO</b>	American Association of State Highway and Transportation Officials
<b>BCP</b>	Business Continuity Plan
<b>CIP</b>	Critical Infrastructure Protection
<b>CMVP</b>	Cryptographic Module Validation Program
<b>COTS</b>	Commercial Off-the-Shelf
<b>CPNI</b>	Centre for the Protection of National Infrastructure
<b>CPU</b>	Central Processing Unit
<b>CSE</b>	Communications Security Establishment
<b>CSRC</b>	Computer Security Resource Center
<b>CSSC</b>	Control System Security Center
<b>CVE</b>	Common Vulnerabilities and Exposures
<b>DCOM</b>	Distributed Component Object Model
<b>DCS</b>	Distributed Control System(s)
<b>DHS</b>	Department of Homeland Security
<b>DMZ</b>	Demilitarized Zone
<b>DNP3</b>	DNP3 Distributed Network Protocol (published as IEEE 1815)
<b>DNS</b>	Domain Name System
<b>DOE</b>	Department of Energy
<b>DoS</b>	Denial of Service
<b>DRP</b>	Disaster Recovery Plan
<b>EAP</b>	Extensible Authentication Protocol
<b>EMS</b>	Energy Management System
<b>EPRI</b>	Electric Power Research Institute
<b>ERP</b>	Enterprise Resource Planning
<b>FIPS</b>	Federal Information Processing Standards
<b>FISMA</b>	Federal Information Security Modernization Act
<b>FTP</b>	File Transfer Protocol
<b>GPS</b>	Global Positioning System
<b>HMI</b>	Human-Machine Interface
<b>HSPD</b>	Homeland Security Presidential Directive
<b>HTTP</b>	Hypertext Transfer Protocol
<b>HTTPS</b>	Hypertext Transfer Protocol Secure
<b>HVAC</b>	Heating, Ventilation, and Air Conditioning
<b>I/O</b>	Input/Output
<b>I3P</b>	Institute for Information Infrastructure Protection
<b>IACS</b>	Industrial Automation and Control System

<b>IAONA</b>	Industrial Automation Open Networking Association
<b>ICCP</b>	Inter-control Center Communications Protocol
<b>ICMP</b>	Internet Control Message Protocol
<b>ICS</b>	Industrial Control System(s)
<b>ICS-CERT</b>	Industrial Control Systems - Cyber Emergency Response Team
<b>IDS</b>	Intrusion Detection System
<b>IEC</b>	International Electrotechnical Commission
<b>IED</b>	Intelligent Electronic Device
<b>IEEE</b>	Institute of Electrical and Electronics Engineers
<b>IETF</b>	Internet Engineering Task Force
<b>IGMP</b>	Internet Group Management Protocol
<b>INL</b>	Idaho National Laboratory
<b>IP</b>	Internet Protocol
<b>IPS</b>	Intrusion Prevention System
<b>IPsec</b>	Internet Protocol Security
<b>ISA</b>	International Society of Automation
<b>ISID</b>	Industrial Security Incident Database
<b>ISO</b>	International Organization for Standardization
<b>IT</b>	Information Technology
<b>ITE</b>	Institute of Electrical Engineers
<b>ITL</b>	Information Technology Laboratory
<b>ITS</b>	Intelligent Transportation Systems
<b>LAN</b>	Local Area Network
<b>M2M</b>	Machine to Machine
<b>MAC</b>	Media Access Control
<b>MES</b>	Manufacturing Execution System
<b>MIB</b>	Management Information Base
<b>MTU</b>	Master Terminal Unit (also Master Telemetry Unit)
<b>NAT</b>	Network Address Translation
<b>NCCIC</b>	National Cybersecurity and Communications Integration Center
<b>NCSD</b>	National Cyber Security Division
<b>NEMA</b>	Formerly the National Electrical Manufacturers Association; now The Association of Electrical Equipment and Medical Imaging Manufacturers
<b>NERC</b>	North American Electric Reliability Council
<b>NFS</b>	Network File System
<b>NIC</b>	Network Interface Card
<b>NISCC</b>	National Infrastructure Security Coordination Centre
<b>NIST</b>	National Institute of Standards and Technology
<b>NSTB</b>	National SCADA Testbed
<b>NTCIP</b>	National Transportation Communications for ITS Protocol
<b>OLE</b>	Object Linking and Embedding
<b>OMB</b>	Office of Management and Budget
<b>OPC</b>	OLE for Process Control
<b>OS</b>	Operating System
<b>OSI</b>	Open Systems Interconnection
<b>PCII</b>	Protected Critical Infrastructure Information



<b>PDA</b>	Personal Digital Assistant
<b>PIN</b>	Personal Identification Number
<b>PID</b>	Proportional – Integral - Derivative
<b>PIV</b>	Personal Identity Verification
<b>PLC</b>	Programmable Logic Controller
<b>PP</b>	Protection Profile
<b>PPP</b>	Point-to-Point Protocol
<b>R&amp;D</b>	Research and Development
<b>RADIUS</b>	Remote Authentication Dial In User Service
<b>RBAC</b>	Role-Based Access Control
<b>RFC</b>	Request for Comments
<b>RMA</b>	Reliability, Maintainability, and Availability
<b>RMF</b>	Risk Management Framework
<b>RPC</b>	Remote Procedure Call
<b>RPO</b>	Recovery Point Objective
<b>RTO</b>	Recovery Time Objective
<b>RTU</b>	Remote Terminal Unit (also Remote Telemetry Unit)
<b>SC</b>	Security Category
<b>SCADA</b>	Supervisory Control and Data Acquisition
<b>SCP</b>	Secure Copy
<b>SFTP</b>	Secure File Transfer Protocol
<b>SIS</b>	Safety Instrumented System
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SNL</b>	Sandia National Laboratories
<b>SNMP</b>	Simple Network Management Protocol
<b>SP</b>	Special Publication
<b>SPP-ICS</b>	System Protection Profile for Industrial Control Systems
<b>SQL</b>	Structured Query Language
<b>SSH</b>	Secure Shell
<b>SSID</b>	Service Set Identifier
<b>SSL</b>	Secure Sockets Layer
<b>TCP</b>	Transmission Control Protocol
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>TFTP</b>	Trivial File Transfer Protocol
<b>TLS</b>	Transport Layer Security
<b>UDP</b>	User Datagram Protocol
<b>UPS</b>	Uninterruptible Power Supply
<b>US-CERT</b>	United States Computer Emergency Readiness Team
<b>USB</b>	Universal Serial Bus
<b>VFD</b>	Variable Frequency Drive
<b>VLAN</b>	Virtual Local Area Network
<b>VPN</b>	Virtual Private Network
<b>WAN</b>	Wide Area Network
<b>XML</b>	Extensible Markup Language

# Glossary

There are a number of glossaries published with definitions of cybersecurity related terms. The National Institute of Science and Technology (NIST) has compiled a **GLOSSARY OF KEY INFORMATION SECURITY TERMS** (NISTIR 7298, Revision 2, May 2013). DHS National Cyber Security Division (NCSA) has compiled a glossary. The National Institute of Cybersecurity Careers and Studies (NICCS), managed by the Cybersecurity Education and Awareness Branch (CEA) within the Department of Homeland Security's (DHS) Office of Cybersecurity and Communications (CS&C), has developed an cybersecurity lexicon intended to complement the NIST Glossary that is located online at <http://niccs.us-cert.gov/glossary>.

## A

Access	The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. (CNSSI 4009)
Access control	The process of granting or denying specific requests for or attempts to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities. (CNSSI 4009)
Access control mechanism	Security measures designed to detect and deny unauthorized access and permit authorized access to an information system or a physical facility. (Adapted from CNSSI 4009)
Active attack	An actual assault perpetrated by an intentional threat source that attempts to alter a system, its resources, its data, or its operations. (Adapted from IETF RFC 4949, NIST SP 800-63 Rev 1)
Active content	Software that is able to automatically carry out or trigger actions without the explicit intervention of a user. (Adapted from CNSSI 4009)
Advanced Persistent Threat (APT)	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). The intention of an APT may be to steal data, or to cause damage to the network or organization, or to plant attack capabilities for future activation. Stuxnet is an example of an ATP. (NIST SP 800-

Air gap	<p>53 Rev 4)                  To physically separate or isolate a system from other systems or networks (verb). The physical separation or isolation of a system from other systems or networks (noun).</p>
Antispyware software	<p>A program that specializes in detecting and blocking or removing forms of spyware.                  (Adapted from NCSD Glossary)</p>
Antivirus software	<p>A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents. Sometimes by removing or neutralizing the malicious code. (Adapted from NCSD Glossary)</p>
Attack or cyber attack	<p>An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. The intentional act of attempting to bypass one or more security services or controls of an information system. (NCSD Glossary. NTSSI 4009 (2000), CNSSI 4009)</p>
Attack method or attack mode	<p>The manner or technique and means an adversary may use in an assault on information or an information system.(Adapted from DHS Risk Lexicon, NCSD Glossary)</p>
Attack path	<p>The steps that an adversary takes or may take to plan, prepare for, and execute an attack. (Adapted from DHS Risk Lexicon, NCSD Glossary)</p>
Attack pattern	<p>Similar cyber events or behaviors that may indicate an attack has occurred or is occurring, resulting in a security violation or a potential security violation. For software, descriptions of common methods for exploiting software systems.                  (Adapted from Oak Ridge National Laboratory Visualization Techniques for Computer Network Defense, MITRE's CAPEC web site)</p>
Attack signature	<p>A characteristic or distinctive pattern that can be searched for or that can be used in matching to previously identified attacks. An automated set of rules for identifying a potential threat (such as an exploit or the presence of an attacker tool) and possible responses to that threat. (Adapted from NCSD Glossary, CNSSI 4009, ISSG V1.2 Database)</p>
Attack surface	<p>The set of ways in which an adversary can enter a system and potentially cause damage.                  An information system's characteristics that permit an</p>

Authentication	<p>adversary to probe, attack, or maintain presence in the information system.</p> <p>The process of verifying the identity or other attributes of an entity (user, process, or device).</p> <p>Also the process of verifying the source and integrity of data. A simple and common authentication procedure is a password. “Two-factor” authentication is the use of two independent forms of authentication, such as a password, a fingerprint, or a series of digits generated by a secure identification token, a small handheld device. (Adapted from CNSSI 4009, NIST SP 800-21, NISTIR 7298)</p>
Authenticity	<p>A property achieved through cryptographic methods of being genuine and being able to be verified and trusted, resulting in confidence in the validity of a transmission, information or a message, or sender of information or a message. (Adapted from CNSSI 4009, NIST SP 800-53 Rev 4)</p>
Authorization	<p>A process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. The process or act of granting access privileges or the access privileges as granted. (OASIS SAML Glossary 2.0; Adapted from CNSSI 4009)</p>
Availability	<p>The property of being accessible and usable upon demand. In cybersecurity, applies to assets such as information or information systems. (Adapted from CNSSI 4009, NIST SP 800-53 Rev 4, 44 U.S.C., Sec 3542)</p>
<b>B</b>	
Backdoor	<p>An undocumented way of gaining access to a computer system. A backdoor is a potential security risk.</p>
Batch Process	<p>A process that leads to the production of finite quantities of material by subjecting quantities of input materials to an ordered set of processing activities over a finite time using one or more pieces of equipment. (ANSI/ISA-88.01-1995)</p>
Behavior monitoring	<p>Observing activities of users, information systems, and processes and measuring the activities against organizational policies and rule, baselines of normal activity, thresholds, and trends.</p>
Blacklist	<p>A list of entities that are blocked or denied privileges or access.</p>

Bot	A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under remote the command and control of a remote administrator. A member of a larger collection of compromised computers known as a botnet.
Bot master or bot herder	The controller of a botnet that, from a remote location, provides direction to the compromised computers in the botnet.
Botnet	A network of computers that have been penetrated, compromised, and programmed to operate on the commands of an unauthorized remote user, usually without the knowledge of their owners or operators. The network of “robot” computers can then be manipulated by the remote actor to commit attacks on other systems. The computers on botnets are frequently referred to as “zombies” and are often employed in digital denial of service attacks.
Broadcast	Transmission to all devices in a network without any acknowledgment by the receivers. (IEC/PAS 62410)
Buffer Overflow	A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Adversaries exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system. (NIST SP 800-28)
Bug	An unexpected and relatively small defect, fault, flaw, or imperfection in an information system or device. (NCSD Glossary)
Build Security In	A set of principles, practices, and tools to design, develop, and evolve information systems and software that enhance resistance to vulnerabilities, flaws, and attacks. (Adapted from Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program (2011), US-CERT's Build Security In website)
<b>C</b>	
Cloud computing	A model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (Adapted from CNSSI 4009, NIST SP 800-145)
Communications Router	A communications device that transfers messages between two

	networks. Common uses for routers include connecting a LAN to a WAN, and connecting MTUs and RTUs to a long-distance network medium for SCADA communication.
Computer network defense	The actions taken to defend against unauthorized activity within computer networks. (CNSSI 4009)
Confidentiality	A property that information is not disclosed to users, processes, or devices unless they have been authorized to access the information. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Adapted from CNSSI 4009, NIST SP 800-53 Rev 4, 44 U.S.C., Sec 3542)
Configuration (of a system or device)	Step in system design; for example, selecting functional units, assigning their locations, and defining their interconnections. (IEC/PAS 62409)
Configuration Control	Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications before, during, and after system implementation. (CNSSI 4009)
Continuous Monitoring	A continuous monitoring program is a process designed to regularly assess information systems to determine if the complete set of planned, required, and deployed security controls within an information system continue to be effective over time, as changes in the system occur. Continuous monitoring transforms the traditional model of static, sporadic security compliance assessments to dynamic, near-real-time situational awareness.
Consequence	The effect of an event, incident, or occurrence. Extended Definition: In cybersecurity, the effect of a loss of confidentiality, integrity or availability of information or an information system on an organization's operations, its assets, on individuals, other organizations, or on national interests. (Adapted from DHS Risk Lexicon, National Infrastructure Protection Plan, NIST SP 800-53 Rev 4)
Continuity of Operations Plan	A document that sets forth procedures for the continued performance of core capabilities and critical operations during any disruption or potential disruption. (Adapted from CPG 101, CNSSI 4009)
Control	The part of the ICS used to perform the monitoring and control of the physical process. This includes all control servers, field

	devices, actuators, sensors, and their supporting communication systems.
Control Center	An equipment structure or group of structures from which a process is measured, controlled, and/or monitored. (ANSI/ISA-51.1-1979)
Control Loop	A control loop consists of sensors for measurement, controller hardware such as PLCs, actuators such as control valves, breakers, switches and motors, and the communication of variables. Controlled variables are transmitted to the controller from the sensors. The controller interprets the signals and generates corresponding manipulated variables, based on set points, which it transmits to the actuators. Process changes from disturbances result in new sensor signals, identifying the state of the process, to again be transmitted to the controller.
Control Network	Those networks of an enterprise typically connected to equipment that controls physical processes and that is time or safety critical. The control network can be subdivided into zones, and there can be multiple separate control networks within one enterprise and site. (ISA99)
Control Server	A controller that also acts as a server that hosts the control software that communicates with lower-level control devices, such as Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs), over an ICS network. In a SCADA system, this is often called a SCADA server, MTU, or supervisory controller.
Control System	A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs and other types of industrial measurement and control systems.
Controlled Variable	The variable that the control system attempts to keep at the set point value. The set point may be constant or variable. (The Automation, Systems, and Instrumentation Dictionary)
Controller	A device or program that operates automatically to regulate a controlled variable. (ANSI/ISA-51.1-1979)
Critical infrastructure	The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters.(Adapted from: National Infrastructure Protection Plan)





Cybercrime	Criminal activity conducted using computers and the Internet, often financially motivated. Cybercrime includes identity theft, fraud, and internet scams, among other activities. Cybercrime is distinguished from other forms of malicious cyber activity, which have political, military, or espionage motivations.
Cyber exercise	A planned event during which an organization simulates a cyber-disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption. (Adapted from NCSG Glossary, DHS Homeland Security Exercise and Evaluation Program)
Cyber incident	Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. (NIST Glossary)
Cyber infrastructure	An electronic information and communications systems and services and the information contained therein. The information and communications systems and services composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. (Adapted from NIPP)
Cybersecurity	The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. (Adapted from CNSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, May 2009)

Cyberspace	The interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (Adapted from NSPD 54/HSPD -23, CNSSI 4009, NIST SP 800-53 Rev 4)
<b>D</b>	
Data aggregation	The process of gathering and combining data from different sources, so that the combined data reveals new information. The new information is more sensitive than the individual data elements themselves and the person who aggregates the data was not granted access to the totality of the information.(Adapted from CNSSI 4009)
Data breach or data leakage	data breach or data leakage The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.
Data Diode	A data diode (also referred to as a unidirectional gateway, deterministic one-way boundary device or unidirectional network) is a network appliance or device allowing data to travel only in one direction.
Data integrity	The property that data is complete, intact, and trusted and has not been modified or destroyed in an unauthorized or accidental manner. (Adapted from CNSSI 4009, NIST SP 800-27)
Data loss	The result of unintentionally or accidentally deleting data, forgetting where it is stored, or exposure to an unauthorized party.
Demilitarized Zone (DMZ)	An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied.(SP 800-41) A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet. (SP 800-45) Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted

sources with restricted access to releasable information while shielding the internal networks from outside attacks.(CNSSI-4009)

Denial of service

An attack that prevents or impairs the authorized use of information system resources or services. A distributed denial of service is a denial of service technique that uses numerous systems to perform the attack simultaneously. (Adapted from NCSD Glossary)

Digital or computer forensics

The processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes. (Adapted fromCNSSI 4009)

Digital Denial of Service (DDOS)

A cyber war technique in which an Internet site, a server, or a router is flooded with more requests for data than the site or device can respond to or process. Consequently, legitimate traffic cannot access the site and the site is in effect shut down. Botnets are used to conduct such attacks, thus distributing the attack over thousands of originating computers acting in unison.

Digital signature

A value computed with a cryptographic process using a private key and then appended to a data object, thereby digitally signing the data. (Adapted from CNSSI 4009, IETF RFC 2828, ICAM SAML 2.0 WB SSO Profile 1.0.2, InCommon Glossary, NIST SP 800-63 Rev 1)

Disruption

An event which causes unplanned interruption in operations or functions for an unacceptable length of time. (Adapted from CNSSI 4009)

## **E**

Encryption

The scrambling of information so that it is unreadable to those who do not have the code to unscramble it.

Enterprise risk management

A comprehensive approach to risk management that engages people, processes, and systems across an organization to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives. Involves identifying mission dependencies on enterprise capabilities, identifying and prioritizing risks due to defined threats, implementing countermeasures to provide both a static

risk posture and an effective dynamic response to active threats; and assessing enterprise performance against threats and adjusts countermeasures as necessary. (Adapted from: DHS Risk Lexicon, CNSSI 4009)

**Event** An observable occurrence in an information system or network. Sometimes provides an indication that an incident is occurring or at least raise the suspicion that an incident may be occurring. (Adapted from CNSSI 4009)

**Exfiltration** The unauthorized transfer of information from an information system. (NIST SP 800-53 Rev 4)

**Exploit** A technique to breach the security of a network or information system in violation of security policy. (Adapted from ISO/IEC 27039 (draft))

**Exposure** The condition of being unprotected, thereby allowing access to information or access to capabilities that an attacker can use to enter a system or network. (Adapted from NCSG glossary)

## **F**

**Failure** The inability of a system or component to perform its required functions within specified performance requirements. (NCSG Glossary)

**Firewall** A capability to limit network traffic between networks and/or information systems. A hardware/software device or a software program that limits network traffic according to a set of rules of what access is and is not allowed or authorized. (Adapted from CNSSI 4009)

## **H**

**Hack** A verb meaning to gain unauthorized access into a computer system.

**Hacker** An unauthorized user who attempts to or gains access to an information system. (CNSSI 4009)

Hactivism	The exploitation of computers and computer networks as a means of protest to promote political ends. The anti-secrecy group Anonymous is an example of a hactivist organization.
<b>I</b>	
Identity and access management	The methods and processes used to manage subjects and their authentication and authorizations to access specific objects.
Incident	An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences. An occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies. (Adapted from CNSSI 4009, FIPS 200, NIST SP 800-53 Rev 4, ISSG)
Incident management	The management and coordination of activities associated with an actual or potential occurrence of an event that may result in adverse consequences to information or information systems. (Adapted from NCSA Glossary, ISSG NCPS Target Architecture Glossary)
Incident response plan	A set of predetermined and documented procedures to detect and respond to a cyber incident. (Adapted from CNSSI 4009)
Indicator	An occurrence or sign that an incident may have occurred or may be in progress. (Adapted from CNSSI 4009, NIST SP 800-61 Rev 2 (DRAFT), ISSG V1.2 Database)
Industrial Control System	<p>computer-based facilities, systems, and equipment used to remotely monitor and/or control critical/sensitive processes and physical functions. These systems collect measurement and operational data from field locations, process and display this information, and, in some systems, relay control commands to local or remote equipment or to human-machines interfaces (operators). (Transportation Industrial Control Systems Cybersecurity Standards Strategy, DHS, 2012)</p> <p>An information system used to control industrial processes such as manufacturing, product handling, production, and distribution or to control infrastructure assets. (Adapted from</p>

NIST SP 800-53 Rev 4, NIST SP 800-82)

Information assurance	The measures that protect and defend information and information systems by ensuring their availability, integrity, and confidentiality. (Adapted from CNSSI 4009)
Information sharing	An exchange of data, information, and/or knowledge to manage risks or respond to incidents. (Adapted from NCSD glossary)
Information system resilience	The ability of an information system to: (1) continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (2) recover effectively in a timely manner. (Adapted from NIST SP 800-53 Rev 4)
Information technology	<p>Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. . . . The term information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware, and similar procedures, services (including support services), and related resources. (40 USC, Sec 11101)</p> <p>Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information. (Adapted from CNSSI 4009, NIST SP 800-53 rev. 4, based on 40 U.S.C. sec. 1401)</p>
Inside(r) threat	A person or group of persons within an organization who pose a potential risk through violating security policies. One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm. (Adapted from: CNSSI 4009; From NIAC Final Report and Recommendations on the Insider Threat to Critical Infrastructure, 2008)

Integrated risk management	The structured approach that enables an enterprise or organization to share risk information and analysis and to synchronize independent yet complementary risk management strategies to unify efforts across the enterprise. (Adapted from DHS Risk Lexicon)
Integrity	The property whereby information, an information system, or a component of a system has not been modified or destroyed in an unauthorized manner. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination. (Adapted from CNSSI 4009, NIST SP 800-53 Rev 4, 44 U.S.C., Sec 3542, SANS; From SAFE-BioPharma Certificate Policy 2.5)
Intent	A state of mind or desire to achieve an objective. (Adapted from DHS Risk Lexicon)
Interoperability	The ability of two or more systems or components to exchange information and to use the information that has been exchanged. (Adapted from IEEE Standard Computer Dictionary, DHS personnel)
Intrusion	An unauthorized act of bypassing the security mechanisms of a network or information system. (Adapted from CNSSI 4009)
Intrusion detection	The process and methods for analyzing information from networks and information systems to determine if a security breach or security violation has occurred. (Adapted from: CNSSI 4009, ISO/IEC 27039 (draft))
<b>K</b>	
Key	The numerical value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.(CNSSI 4009)
Key pair	A public key and its corresponding private key. Two mathematically related keys having the property that one key can be used to encrypt a message that can only be decrypted using the other key. (Adapted from CNSSI 4009, Federal Bridge Certificate Authority Certification Policy 2.25)
Keylogger or keystroke logger	Software or hardware that tracks keystrokes and keyboard events, usually surreptitiously / secretly, to monitor actions by

the user of an information system. Cybercriminals install them on computers to clandestinely record the computer user's passwords and other confidential information.

## L

### Logic bomb

A software application or series of instructions that cause a system or network to shut down and/or to erase all data or software on the network. A logic bomb is a type of malware.

## M

### Macro virus

A type of malicious code that attaches itself to documents and uses the macro programming capabilities of the document's application to execute, replicate, and spread or propagate itself. (Adapted from CNSSI 4009)

### Malicious applet

A small application program that is automatically downloaded and executed and that performs an unauthorized function on an information system. (CNSSI 4009)

### Malicious code

Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system. Includes software, firmware, and scripts. (Adapted from CNSSI 4009, NIST SP 800-53 Rev 4)

### Malicious logic

Hardware, firmware, or software that is intentionally included or inserted in a system to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system. (Adapted from CNSSI 4009)

### Malware

Software that compromises the operation of a system by performing an unauthorized function or process. (Adapted from CNSSI 4009, NIST SP 800-83)

### Mitigation

The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences. Implementing appropriate risk-reduction controls based on risk management priorities and analysis of alternatives. (Adapted from DHS Risk Lexicon, CNSSI 4009, NIST SP 80)



## N

- Network resilience** The ability of a network to: (1) provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged); (2) recover effectively if failure does occur; and (3) scale to meet rapid or unpredictable demands. (Adapted from CNSSI 4009)
- Network Services** Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.
- Non-repudiation** A property achieved through cryptographic methods to protect against an individual or entity falsely denying having performed a particular action related to data. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.  
(Adapted from CNSSI 4009; From: NIST SP 800-53 Rev 4)

## O

- Object** A passive information system-related entity containing or receiving information. (Adapted from CNSSI 4009, NIST SP 800-53 Rev 4)
- Outside(r) threat** A person or group of persons external to an organization who are not authorized to access its assets and pose a potential risk to the organization and its assets. (Adapted from CNSSI 4009)

## P

- Passive attack** An actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations. (Adapted from IETF RFC 4949, NIST SP 800-63 Rev 1)

Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. (FIPS 140-2)
Pen test or penetration testing	An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system. (Adapted from NCSD Glossary, CNSSI 4009, NIST SP 800-53 Rev 4)
Personal Identifying Information / Personally Identifiable Information	The information that permits the identity of an individual to be directly or indirectly inferred. (Adapted from NCSD Glossary, CNSSI 4009, GAO Report 08-356, as cited in NIST SP 800-63 Rev 1)
Pharming	A technique used by hackers to redirect users to false websites without their knowledge.
Phishing	A digital form of social engineering to deceive individuals into providing sensitive information such as usernames, passwords, social security numbers and credit card details. Common phishing tactics include posing as a known contact, a legitimate company, or an otherwise trusted entity in an electronic communication. (Adapted from NCSD Glossary, CNSSI 4009, NIST SP 800-63 Rev 1)
Plaintext	Unencrypted information.(CNSSI 4009)
Precursor	An observable occurrence or sign that an attacker may be preparing to cause an incident. (Adapted from CNSSI 4009, NIST SP 800-61 Rev 2 (DRAFT))
Privacy	The assurance that the confidentiality of, and access to, certain information about an entity is protected. The ability of individuals to understand and exercise control over how information about themselves may be used by others. (NIST SP 800-130)
Private key	A cryptographic key that must be kept confidential and is used to enable the operation of an asymmetric (public key) cryptographic algorithm. The secret part of an asymmetric key pair that is uniquely associated with an entity. (Adapted from CNSSI 4009, NIST SP 800-63 Rev 1, FIPS 201-2, FIPS 140-2, Federal Bridge Certificate Authority Certification Policy 2.25)
Public Key Infrastructure	A framework consisting of standards and services to enable secure, encrypted communication and authentication over potentially insecure networks such as the Internet. A framework and services

for generating, producing, distributing, controlling, accounting for, and revoking (destroying) public key certificates. (Adapted from CNSSI 4009, IETF RFC 2828, Federal Bridge Certificate Authority Cross-certification Methodology 3.0, InCommon Glossary, Kantara Identity Assurance Framework 1100, NIST SP 800-63 Rev 1)

## R

Recovery	The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term. (Adapted from NIPP)
Redundancy	Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process. (DHS Risk Lexicon)
Response	The activities that address the short-term, direct effects of an incident and may also support short-term recovery. In cybersecurity, response encompasses both automated and manual activities. (Adapted from National Infrastructure Protection Plan, NCPS Target Architecture Glossary)
Risk	The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences. (Adapted from: DHS Risk Lexicon, NIPP and adapted from CNSSI 4009, FIPS 200, NIST SP 800-53 Rev 4, SAFE-BioPharma Certificate Policy 2.5)
Risk assessment	The product or process which collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making. The appraisal of the risks facing an entity, asset, system, or network, organizational operations, individuals, geographic area, other organizations, or society, and includes determining the extent to which adverse circumstances or events could result in harmful consequences. (Adapted from DHS Risk Lexicon, CNSSI 4009, NIST SP 800-53 Rev 4)
Risk-based data management	A structured approach to managing risks to data and information by which an organization selects and applies appropriate security controls in compliance with policy and commensurate with the sensitivity and value of the data.
Rootkit	A set of software tools with administrator-level access privileges installed on an information system and designed to hide the presence of the tools, maintain the access privileges, and conceal

the activities conducted by the tools. (Adapted from CNSSI 4009)

## S

Security policy	A rule or set of rules that govern the acceptable use of an organization's information and services to a level of acceptable risk and the means for protecting the organization's information assets. A rule or set of rules applied to an information system to provide security services.(Adapted from CNSSI 4009, NIST SP 800-53 Rev 4, NIST SP 800-130, OASIS SAML Glossary 2.0)
Situational awareness	Comprehending information about the current and developing security posture and risks, based on information gathered, observation and analysis, and knowledge or experience. In cybersecurity, comprehending the current status and security posture with respect to availability, confidentiality, and integrity of networks, systems, users, and data, as well as projecting future states of these. (Adapted from CNSSI 4009, DHS personnel, National Response Framework)
Software assurance	The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle, and that the software functions in the intended manner. (CNSSI 4009)
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. (Adapted from CNSSI 4009)
Spoofing	Faking the sending address of a transmission to gain illegal [unauthorized] entry into a secure system. The deliberate inducement of a user or resource to take incorrect action. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing. (CNSSI 4009)
Spyware	Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner. (Adapted from CNSSI 4009, NIST SP 800-53 Rev 4)
Supervisory Control and Data Acquisition (SCADA)	A generic name for a computerized system that is capable of gathering and processing data and applying operational controls to geographically dispersed assets over long distances. (Adapted from NCSD Glossary, CNSSI 4009)

**System integrity** The attribute of an information system when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system. (CNSSI 4009)

**T**

**Threat** A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society. Includes an individual or group of individuals, entity such as an organization or a nation), action, or occurrence. (Adapted from DHS Risk Lexicon, NIPP, CNSSI 4009, NIST SP 800-53 Rev 4)

**Threat actor or threat agent** An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (Adapted from DHS Risk Lexicon)

**Threat analysis** The detailed evaluation of the characteristics of individual threats.

**Threat assessment** The product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property. (From DHS Risk Lexicon and adapted from CNSSI 4009, NIST SP 800-53, Rev 4)

**Traffic light protocol** A set of designations employing four colors (RED, AMBER, GREEN, and WHITE) used to ensure that sensitive information is shared with the correct audience. (Adapted from US-CERT)

**Transportation infrastructure** Travel ways (e.g., pavements or fixed guideways such as rails), structures (e.g., bridges, tunnels, plazas and buildings), fixtures and appurtenances (e.g., signals, signs, sensors, gates, controllers and computers) and rolling stock (e.g., transit vehicles and support service vehicles).

**Trojan horse** A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (CNSSI 4009)

## U

**Unauthorized access** Any access that violates the stated security policy. (CNSSI 4009)

## V

**Virus** A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer. (Adapted from CNSSI 4009)

**Vulnerability** A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard. Characteristic of location or security posture or of design, security procedures, internal controls, or the implementation of any of these that permit a threat or hazard to occur. (Adapted from DHS Risk Lexicon, CNSSI 4009, NIST SP 800-53 Rev 4)

**Vulnerability Assessment and Management** In cybersecurity work where a person conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations, enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

## W

**Weakness** A shortcoming or imperfection in software code, design, architecture, or deployment that, under proper conditions, could become a vulnerability or contribute to the introduction of vulnerabilities. (Adapted from ITU-T X.1520 CWE, FY 2013 CIO FISMA Reporting Metrics)

**Whitelist** A list of entities that are considered trustworthy and are granted access or privileges.

Work factor	An estimate of the effort or time needed by a potential adversary, with specified expertise and resources, to overcome a protective measure. (Adapted from CNSSI 4009)
Worm	A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself. (CNSSI 4009)
<b>Z</b>	
Zero-day Attack	A cyberattack that uses previously unknown coding (malware, etc.) or exploits a previously unknown security vulnerability. This type of attack is particularly dangerous because existing patches, anti-virus software, and other defenses are not programmed to defend against it. It is called a zero-day attack, because it occurs on “day zero” of learning of the vulnerability.
Zombie	Computers on botnets are frequently referred to as “zombies” and are often employed in digital denial of service attacks.