APTA STANDARDS DEVELOPMENT PROGRAM

RECOMMENDED PRACTICE

American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215

APTA SS-ECS-RP-001-14

Approved October 17, 2014

Enterprise Cyber Security Working Group

Cybersecurity Considerations for Public Transit

Abstract: This *Recommended Practice* establishes considerations for public transit chief information officers (CIOs) interested in developing cybersecurity strategies for their organizations. It details practices and standards that address vulnerability assessment and mitigation, system resiliency and redundancy, and disaster recovery.

Keywords: advanced persistent attacks, cyber, cybersecurity assessments, cyberassets, disaster recovery, enterprise cybersecurity, fallback, information security (INFOSEC), information and communication technology (ICT), information security, intrusion detection, redundancy, resiliency, secure cloud, system penetration

Summary: Cybersecurity is a growing concern for public transit managers, as control and management systems become increasingly dependent on information technology. These systems are vulnerable to increasingly sophisticated direct and indirect cyberattacks. The typical transit-based IT infrastructure is comprised of a complex and interconnected series of components, subcomponents and services. This complexity increases the exposure of these systems to threats. Given these increasing risks, the transit industry and its technology managers must take proper steps to ensure the security of their cybersystems.

Scope and purpose: The purpose of this document is to provide information on and considerations for cybersecurity within the public transit enterprise. This document is not a substitute for a cybersecurity program. Nothing in this document should be taken to contradict standards and guidelines made mandatory by local, state or federal governments.

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Enterprise Cyber Security Working Group**, which provided the primary effort in the drafting of this *Recommended Practice*.

At the time this standard was completed, the working group included the following members:

Lurae Stewart

Michael Bosche

Theodore Lawrence

Gary Foster

Brad Baker
Aida Asuncion
Michael DePallo
Lee Allen
Barry Einsig
Sean Ryan
Dave Gorshkov
David Hahn
Doug Hawkins
John Hogan
Lisa Kaiser
Joseph Kelly
John Plante
Josh Poster
Sean Ryan
Harry Saporta
Dave Teumim
John Walsh
Derrick Wigglesworth
Bridget Zamperini
John Zukosky

Contents

Cybersecurity Considerations for Public Transit

1. Overview

Cybersecurity is a growing concern that all transit agencies from large to small must recognize and take appropriate actions on. With the unprecedented pace and complexity of cyberattacks, a transit agency must be proactive and adopt a holistic approach at the strategic level to protect its organization's critical information and fulfill its obligation to its customers. Cybervulnerabilities are exploited not only directly by means of information technology (IT), but the threat also has grown to a level of sophistication in which social engineering has been leveraged to exploit individuals. A transit agency's cybersecurity strategy must be tightly woven into the fabric of the organization at all levels. While eliminating cyberthreats is impossible, transit agencies must take a full-spectrum risk-based approach. No longer is cybersecurity an IT department problem. It has manifested to become a critical management issue that requires some aspect of involvement at the highest level.

The American Public Transportation Association has developed several working groups to address the serious concern of cybersecurity. The mandate of these working groups is to produce guidance in maintaining adequate cybersecurity that all transit agencies, large or small, can utilize and implement. This document is a headway into a family of specific cybersecurity related *Recommended Practices*. This document specifically is meant to provide transit agencies an overview of cybersecurity considerations. Other *Recommended Practices* that transit agencies can adopt and tailor for their immediate use are linked and referenced throughout.

1.1 National cybersecurity strategy

The dependence on and seamless integration of technology into everyday activities and operations has exposed and brought to the forefront the critical need to address cybersecurity. APTA understands the real cyberthreats against transit infrastructure and agencies across the nation. Cyberthreats have become such an important and sensitive concern that the current administration has identified cybersecurity as an important priority. The administration's cybersecurity strategy is twofold:

- **Improve resilience to cyber-incidents** by hardening digital infrastructure to be more resistant to penetration and disruption; improving the ability to defend against sophisticated and agile cyberthreats; and recovering quickly from incidents, whether caused by malicious activity, accident or natural disaster.
- **Reduce the cyberthreat** through working with allies on international norms of acceptable behavior in cyberspace, strengthening law enforcement capabilities against cybercrime and deterring potential adversaries from taking advantage of remaining vulnerabilities.

To support and achieve the goals of the nation's cybersecurity strategy, and aligning with the Department of Homeland Security (DHS), the Department of Transportation (DOT) and the Transportation Security Administration (TSA), APTA has broadly identified the following priorities for transit agencies to consider and at the minimum address with respect to an agency's information and communication technology (ICT) infrastructure. The four priorities represent a broad-based, balanced information security program that

addresses the management, operational and technical aspects of protecting federal information and information systems:

1. **Standards, policies and procedures:** Transit agencies should develop, formalize and document thorough standards, policies and procedures in protecting against cyberthreats and improving resilience to such incidents.
2. **Information system technology and infrastructure:** Transit agencies should ensure the capability, maintenance, serviceability and interoperability of the organization's ICT infrastructure. Transit agencies should implement a thorough system development life cycle (SDLC) process that integrates risk management into the process.
3. **Awareness, training and education:** Transit agencies should focus on developing a general culture of awareness on cybersecurity. Further, transit agencies should identify specific individuals necessary to receive further training and education as part of their professional development and career progression, to enhance the organization's internal capabilities against cyberthreats.
4. **Information security risk management integration:** Transit agencies should integrate information security into the organization's risk management strategy from the very top to align with the organization's strategy, mission and goals. Integrating information security into the risk management process will ensure proper identification and allocation of essential resources in enhancing the organization's ability to mitigate increase resiliency against cyberattacks.

1.2 Transportation systems sector cybersecurity strategy

Our national security depends on an open, reliable and secure transportation system. The sector's cyberinfrastructure, which includes both business systems and physical automation systems, plays a critical role, as it enables increasingly complex and technologically sophisticated transportation operations. The sector's cybersystems and physical automations require protection against malicious and inadvertent manipulation. Due to the numerous interdependencies within the sector, failure to protect these systems and automations may result in significant and adverse business, safety and security implications throughout the sector. By maintaining continuous cybersecurity awareness, improving and expanding voluntary participation, defining the conceptual environment, enhancing intelligence and security information sharing, and ensuring sustained coordination and strategic implementation, transit agencies should be able to deter significant threats and to help protect their systems.

2. Cyberthreat landscape

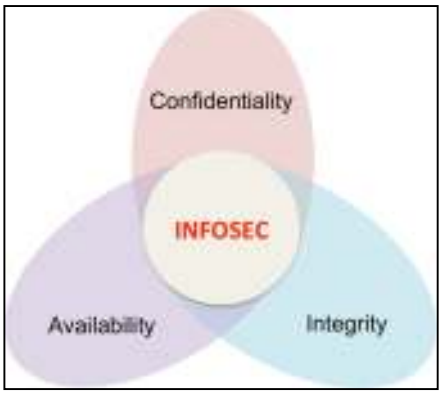
2.1 Target

With the growing dependence on information and communication technology by governments, business, individuals and the networks linking to the end users, cyberspace is increasingly becoming an attractive target. An effective cyberattack against a transportation agency will seek to compromise the **confidentiality**, **availability** and/or **integrity** (see **Figure 1**) of the agency's information by of exploiting the enterprise's ICT system:

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

- **Availability:** Ensuring timely and reliable access to, and use of, information. A loss of availability is the disruption of access to or use of information or an information system.
- **Integrity:** Guarding against improper information modification or destruction; this includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

FIGURE 1
Information Security Diagram



Modern transit systems are heavily dependent on a variety of information technology systems and therefore are naturally "at risk" to a wide spectrum of cyberthreats. Cyberattacks can destroy a transit agency's physical systems, render them inoperable, hand over control of those systems to an outside entity or jeopardize the privacy of employee or customer data. Cyberattacks threaten every aspect of modern life that is touched—indirectly or directly—by information technology.

Typically, a transportation agency's IT infrastructure consists of three general layers (see **Figure 2**): operational systems, enterprise information systems and subscribed systems. These layers are integrated and implicitly dependent on one another for seamless operations. Each layer is critical to the operational integrity of the transit agency and—for the purposes of this *Recommended Practice*—will be referred to as the transportation information ecosystem (TI ecosystem), as a whole. Systems within the TI ecosystem may share or depend upon data stored and processed within other layers.

FIGURE 2
Transportation Information Ecosystem

Cyberattacks may exploit and target specific system layers within the transit agency, including but not limited to the following:

- **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.

2.2 Threats

Cyberspace is a unique ambiguous environment that easily allows governments, criminals, terrorists and even mischievous juveniles to mask their identity and remain anonymous. Cyberattacks directed against transportation organizations can be conducted in many forms, which may consist of a single act or a combination of discrete steps threaded together. Such acts may be a complicated exploitation of coding or the simple use of social engineering—an art of manipulating individual's trust, behavior or identity—to reveal or to gain access to confidential information. Once the targeted system is compromised, perpetrators might implement "back door" gates or install stealth code allowing information to be monitored or removed without detection. "Zero day" switches can be implemented, which can be activated at a specified time or under a specified set of conditions, turning control of the operational or business systems over to the perpetrator.

Furthermore, cyberthreats may not all be software attacks. While cyberattacks in the form of software manipulation require a degree of expertise and technical knowledge, physical manipulation (intentional and unintentional) of the system is of real concern as well. Many attacks are known to exploit specific hardware linked to the TI ecosystem. Such examples may include manipulation of infrared (IR) or laser signaling devices, jamming Wi-Fi signals or even physical tapping or damaging critical communication cabling or nodes.

Successful cyberattacks rarely take the same form in consecutive or follow-on assaults against a targeted system. The cyberenvironment is in its fastest form of evolution, with exponential advancements of technology and information sharing. Due to the "arms race" culture that exists in the initiating elements (criminal organizations, state actors, activists or "hacktivists") and the mitigating or responding elements (government, industry and law enforcement), attacks are adapted in response to the level of success or failure with which they impact a target organization. Cyberattacks that are detected are usually contained and/or mitigated through some form of countermeasure or response. These countermeasures force the initiating elements to evolve their attack in order to circumvent the countermeasures. Many of the most threatening cyberattacks are now designed to hide in the system and evade detection, quarantine and/or removal; by gaining control of the software that is implemented to capture the malicious software (called *malware)* in the first place. Additionally, such sophisticated malware is capable of regular self-updates, prolonging survivability and preventing detection. (e.g., Stuxnet).

While many cyberattacks may be external, transit agencies, just like any other organization, are susceptible to attacks from internal sources, such as a disgruntled employee. An attack from an internal source has a higher probability of success and a greater potential for damage, given the level of access and knowledge an insider may possess. Employees with minimal constraints or supervision can cause significant damage and pose a serious threat to a transit agency.

Cyberthreats and vulnerabilities of critical components of the transportation information ecosystem not only put the transit agency and the lives of passengers at risk but may also put the agency in noncompliance with many legal requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), payment card industry (PCI) security standards and the Patriot Act. Compromise of the ICT systems not only puts confidentiality at risk, but also threatens the integrity and availability of the functions of the transit agency. Cyberattacks pose a serious threat with detrimental consequences to any modern transit agency.

Transit agencies must be proactive and approach cybersecurity risks with a holistic solution that involves effective strategy addressing the three key areas of IT infrastructure: operations, people and facilities.

Additionally, transit agencies must rely on collaborative forums that enable knowledge sharing to promote awareness of new attacks, particularly industry-specific attacks. Raising awareness about the potential risks will improve the overall vigilance that an agency applies to these threats. Cyberthreats to transportation systems will only increase with time.

3. Transportation information ecosystem

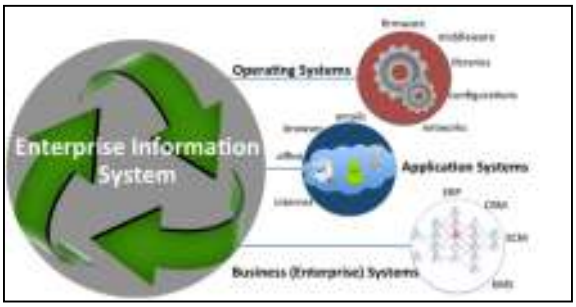
The TI ecosystem is comprised of layers of systems that perform various functions that allow the transit agency to deliver services to its customers (see **Figure 2**). These layers are interconnected, working in concert and sharing data among the layers. While each layer must be secured and protected, special attention is needed with interface and connectivity between layers. The links between layers often are the most vulnerable and easiest way to gain access into the TI ecosystem. (e.g., through the transit agency website to access stored data containing specific SCADA configurations.)

3.1 Operational systems

Operational systems in a transit agency include SCADA, train controls and other operational systems. A common misconception is that SCADA systems are not vulnerable to cybersecurity attacks given that such systems are not directly linked to the World Wide Web and typically do not have a graphical user interface (GUI). While it is true that early SCADA systems were designed and built on separate networks and controls, advancements in IT infrastructure and the evolution of information management practices required that the link between SCADA and enterprise systems be bridged. Much attention has been placed on the vulnerabilities of SCADA-based systems in recent times because of their ubiquitous implementation footprint in multiple industries and the lengthy record of effective operations. Additionally, much of the early security designs utilize outdated digital and analog technology. Some SCADA-based systems have been in operation since the 1970s, and many of the particulars (i.e., architecture and technical controls) of such systems are readily available online. SCADA security controls are archaic, simple and poorly designed. Furthermore, methods to exploit security vulnerabilities and gaps of specific SCADA systems are documented online by many underground hacking organizations or individuals.

3.2 Enterprise information system

FIGURE 3
Enterprise Information System



The enterprise information system (EIS) is the overall information management system that manages the agency's information technology platform to support the organization. EIS integrates core functions of the organization and can be broadly layered into three subcategories: operating systems, application systems and business systems.

- **Operating systems** are the core backbone of the information infrastructure system. They serve as the common platform to manage the entire hardware resources necessary for a specific applications system. Such resources include processor time, memory allocation, network communication, etc.
- **Applications systems** primarily consist of the user-interfaced software. Such software may be comprised of proprietary software, third-party software or bundled software from the operating system. Application systems are often considered at the highest risk to cyberattacks, particularly networking-capable applications, such as email and web browser applications.
- **Business (enterprise) systems** are a form of specialized applications specifically responsible for managing the agency's confidential information and day-to-day business functions. Such systems

include enterprise resource planning (ERP), customer relationship management (CRM), knowledge management system (KMS), and supply chain management (SCM).

Because the three systems are layered and integrated, vulnerabilities and/or configuration errors within any layer will expose other systems to potential intruders, compromising the entire system. It is most likely that an indirect vulnerability will be exploited in order to gain access to various levels of the transportation information ecosystem. In particular, according to SANS Institute in 2009, applications systems vulnerabilities exceed operating system vulnerabilities, which results in a more highly concentrated focus of exploitation attempts, specifically through web-based applications. In order to protect the health of a transit agency's enterprise information system, two basic priorities can dramatically lead to a more resilient and secure system:

- **Enterprise software and firmware updates:** With the constant evolution of cyberthreats and attacks, developers, vendors and third-party security agencies are constantly providing updated software and firmware updates. By staying up to date, agencies will be armed with the latest patches and tools to prevent cyberattacks from current threats.
- **Web-interfacing applications:** Any applications and connections to external networks should be configured to maximize unauthorized connections and access. Such configurations must include but are not limited to firewall protection, closing unnecessary port access, authentication and utilizing secure socket layer (SSL) connection, and monitoring data exchange.

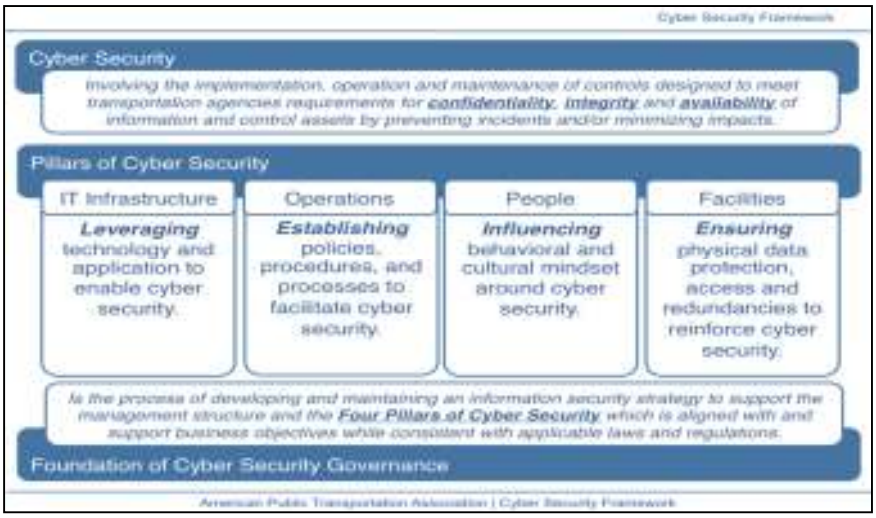
3.3 Subscribed system

Many transit agencies are reliant on subscribed systems to access and manage external resources and data. Such managed services may include financial transactions, support systems maintenance, payroll, customer and employee data, and much more. It is important to note that many transit agencies are subject to meet specific federal, state and local information security mandates and directives, while providers of such subscribed systems may not be. Transit agencies must ensure that third-party vendors are compliant and meet specific information security requirements. Furthermore, transit agencies need to have a well-working relationship with third-party vendors, with processes and procedures in place that facilitate specific action plans in the event of a cybersecurity incident. Such plans must be reviewed, exercised and updated on a regular basis.

4. Pillars of cybersecurity

Transportation organizations should consider the four domains of cybersecurity when developing their information security (INFOSEC) strategies. These domains are considered the key pillars to enhancing a transit agency's cybersecurity capability and resiliency. They include IT infrastructure, operations, people and facilities. The pillars are designed to achieve information security through maintaining **confidentiality**, preserving **integrity**, and sustaining **availability**. While each of the pillars makes an individual contribution to strengthening information security, it is the mutual support from the other pillars that provides a fully effective security shield in protecting the transit agency. No pillar in isolation can achieve such security. In addition, transit agencies must identify appropriate security levels within each layer of the TI ecosystem. A cybersecurity framework (**Figure 4**) has been identified for transit agencies to adopt and utilize; however, it is just one of many existing models.

FIGURE 4
Cybersecurity Framework



4.1 Governance

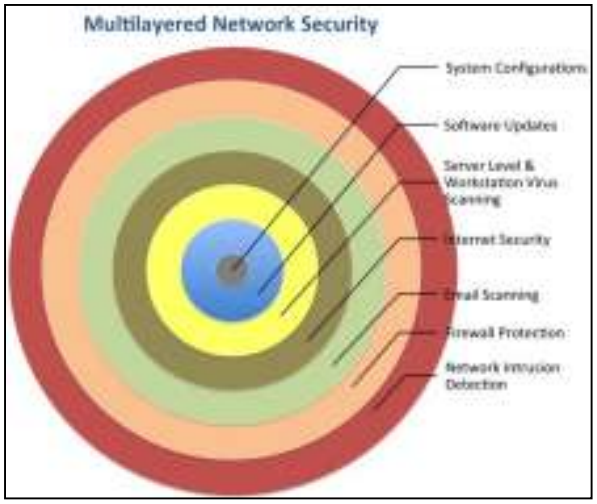
It is a common misconception that cybersecurity can be achieved through IT alone. Effective security must be holistic and requires active participation from senior management, coupled with risk management, accountability and reporting. Governance is the foundation that guides and supports the pillars of cybersecurity, while steering individual transit agencies through their obligations to protect, secure and control critical information. Governance identifies the desired end state for the transit agency to achieve, while ensuring that such strategies are aligned and implemented. Through a consistent and uniform approach, governance is channeled to support each of the pillars to ensure coherence across all the elements of cybersecurity. Transit agencies should consider adopting and developing an information security governance framework. An information security governance framework will embed cybersecurity into transit agencies' corporate governance process.

4.2 IT infrastructure

IT infrastructure is a critical supporting element that the transit agency depends on to facilitate information exchange and is more technical by nature. IT infrastructure is broadly divided into three codependent segments of hardware, software and configuration. Network security is greatly dependent on the working relationships among all three, and a multilayered approach should be taken to maximize efforts by all three segments working together. **Figure 5** shows an example of utilizing hardware, software and configurations to implement multilayered network security. Transit agencies must regularly evaluate their complete IT infrastructure and consider three aspects:

- **Configuration:** Specific IT system management/control between hardware and hardware, hardware and software, and software

FIGURE 5
Example of a Multilayered Network Security



and software. Specific configurations will create more secure IT environment while having the capability to create redundancies within the system, further enhancing the system for other functions, such as intrusion detection and data recovery. Such configuration considerations may include configuration management database, access control management and firewall configuration.

- **Hardware:** All aspects of IT infrastructure in the physical sense are considered hardware, from servers and Wi-Fi access points to USB drives. Hardware advancements are creating smarter, faster, smaller and more secure equipment. It is essential for transit agencies to implement hardware acquisition lifespan management in order to maximize the utility of advanced technology, particularly security. Acquisition lifespan management will allow transit agencies to determine IT requirements, identify alternatives, select suitable solutions, integrate new solutions, maintain current operations and properly phase out legacy systems. Newer edge type hardware creates additional concerns related to the security of a network. Never before have so many data-jacks been installed in public areas. Anything from a telephone to a surveillance camera may be directly connected to a network and additional considerations need to be made in the form of physical security and device monitoring to deter and prevent cybercrime.
- **Software:** The platform that not only interfaces with end users but also controls, manipulates and accesses information through hardware. Software can be an easy target, particularity new versions of software, which can more easily be exploited through the software coding. Software security exploitation and security patching is a never-ending battle. Thus, transit agencies must keep up to date with the latest software updates to address specific security gaps as they are discovered. OEM firmware updates and software updates are not enough; security software should be deployed as part of the transit agency's cybersecurity defense, such as logging systems, antivirus, vulnerability management tools etc.

4.3 Operations

Operations manages the policies, procedures and processes in which transit agencies will implement, enforce and achieve cybersecurity. Policies, procedures and processes establish the necessary structures and boundaries within the transit agency. This structured approach will provide direction and guidance to transit agencies, which will address a host of concerns. It is imperative for transit agencies to publish, communicate and enforce policies, procedures and processes in order to support and enable the pillars of cybersecurity. In doing so, transit agencies will have the capability to be proactive and reactive to cybersecurity related threats and incidents. Additionally, established policies, procedures and processes will minimize the potential risk to social engineering, information exploitation, internal threats, etc. Such plans must be reviewed, exercised and updated on a regular basis. At a minimum, transit agencies should have the following policies and procedures to manage the organization's ICT use and cybersecurity:

- **The INFOSEC plan** aligns with the transit agency's cybersecurity strategy and communicates to the organization specific control measures of policies, procedures and processes in order to meet the cybersecurity needs of the transit agency. An INFOSEC plan supports routine and non-routine (emergency) cybersecurity-related activities, helping to reduce the impact on business operations, information and system assets, and employees. The INFOSEC plan must be regularly reviewed, updated and accepted through a process of security certification and accreditation, which is directly linked to the risk-management process. An INFOSEC plan will document all guidance related to information security, such as incident response, network security, access control, gateway security, communications security, personnel security, physical security, accreditations and certifications, etc.
- **Employee ICT standard operating procedures** document specific procedures for employees' individual conduct, use and access to transit agency ICT hardware, software, data and networks. ICT procedures must clearly document required expectations and be empowered by specific

consequences. Additionally, employees should be required to sign an abiding employee ICT end user agreement to further and legally reinforce employees' obligation and compliance.

4.4 People

Regardless of the level or amount of technology deployed as part of any security system, it is the human element that will remain the weakest link in any security system. It is difficult to predict the intent of the human mind or to determine one's motives. However, transit agencies can build a culture of awareness within the organization, creating like-minded individuals to further support and be supported by the other pillars. Furthermore, this will achieve a more secure information security environment. Building a culture of awareness and further enhancing cybersecurity capabilities will consist of three primary areas (**Figure 6**):

FIGURE 6
Professional Development Ladder

- **Education** integrates all the security skills and competencies of various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues and principles. Information security education strives to produce information security specialists and professionals who are capable of vision and proactive responses.
- **Training** aims to produce relevant and needed security knowledge and skills within the workforce. Training supports professional development and assists personnel in performing their security roles, as outlined by their duties and responsibilities. The most important difference between training and awareness is that training seeks to teach skills that allow an individual to perform a specific function at a certain level of competency, while awareness seeks to focus an individual's attention on an issue or a set of issues. Awareness and training normally involve all the staff of a given organization.
- **Awareness** is a blended solution of activities that promote security, establish accountability, and inform the workforce. An awareness program includes a variety of tools of communication, outreach and metrics development. Awareness programs continually push and reinforce security themes to users in a variety of formats and provide them security information. The first part of addressing awareness is to introduce concepts of responsibility, expectations and accountability as a platform on which to develop the necessary skills.

Awareness and training programs must be designed to incorporate the mission, goals and objectives outlined in the information security strategic plan, if one exists.

4.5 Facilities

Not all cyberthreats and attacks are from digital, software or network manipulation. Many attacks come in the form of compromising physical hardware of an organization's ICT infrastructure. Transit agencies must assess six major areas of physical and environmental security controls with respect to the transportation information ecosystem in which the organization is able to protect against Internet Service Provider interruptions, physical damage, unauthorized disclosure/access, loss of system integrity, and theft. The six major areas identified are areas of concern to evaluate from a perspective of securing transit agencies' physical ICT hardware. Transit agencies should refer to all federal, state and local requirements with respect to safety and security and ensure compliance of physical structures and facilities.

- **Access control:** Unauthorized access to a transit agency's information network or premises places the whole organization at risk. Physical access control should not be limited to physical hardware storage but needs to extend and include location of communication transmission wires, electric power sources, HVAC and any other resources possessing a link to ICT infrastructure.
- **Fire safety:** Building fires are a significant threat, and prevention is of high importance. Fires have the potential to take human life, as well as complete destroy hardware and data. Transit agencies must evaluate the fire safety of the physical environment and develop plans to mitigate potential losses in the event of a fire.
- **Supporting utilities:** Failures in heating and air conditioning systems and electricity services may cause service interruption and damage equipment. Transit agencies identify and implement redundancies to ensure uninterrupted service.
- **Building structure:** Natural disasters may weaken and compromise the safety of the building. Transit agencies need to develop contingency plans to identify alternative locations for business operations and information security.
- **Interception of data:** Data may be intercepted, posing a significant risk to any transit agency. Data interception could occur through direct observation, interception of transmission or electromagnetic interception (i.e., Wi-Fi).
- **Portable media:** Viruses, worms and other malware that are used to exploit an information system may be carried on portable media. Such portable media are easily concealed and pose a significant risk to any transit agency. Transit agencies should treat portable media as a controlled object and implement policies and procedures in authorizing the use and transportation and use of portable media with their IT equipment.

5. Managing information security risk

This section presents an overview of the significance of managing information security risk within the organization, based on key concepts and principles established by the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST). Comprehensive and thorough risk management processes are published by ISO; see Section 8 for further reference.

An effective and robust information security program must implement a robust risk management process. In terms of organizational risk management, the primary goal of any organization is to protect the organization, continue operations and minimize unnecessary liabilities. However, historically the views of information security often have been viewed as a technical process to be left out of the scope of the risk management process. Such practices often provided limited perspective and left the organization vulnerable because of inadequate resources allocated to information security. Therefore, the risk management process of information security must not be viewed as a technical task but must be an essential management function of the organization. Information security should be incorporated into the larger context of the risk-management strategy, achieving the organization's strategy, mission and goals.

As defined by NIST, the objective of information security is the following:

- Ensure that senior leaders/executives recognize the importance of managing information security risk and establish appropriate governance structures for managing such risk.
- Ensure that the organization's risk-management process is being effectively conducted across the three tiers of organization, mission/business processes and information systems.
- Foster an organizational climate where information security risk is considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture and system development life cycle processes.

- Help individuals with responsibilities for information system implementation or operation better understand how information security risk associated with their systems translates into organization-wide risk that may ultimately affect the mission/business success.

The successful implementation of information security objectives is heavily dependent on senior leadership, in such that risk management must be a core function of the organization. Senior leadership must take ownership of the process to implement and manage an effective risk-management program. Effectively managing information security risk requires the following:

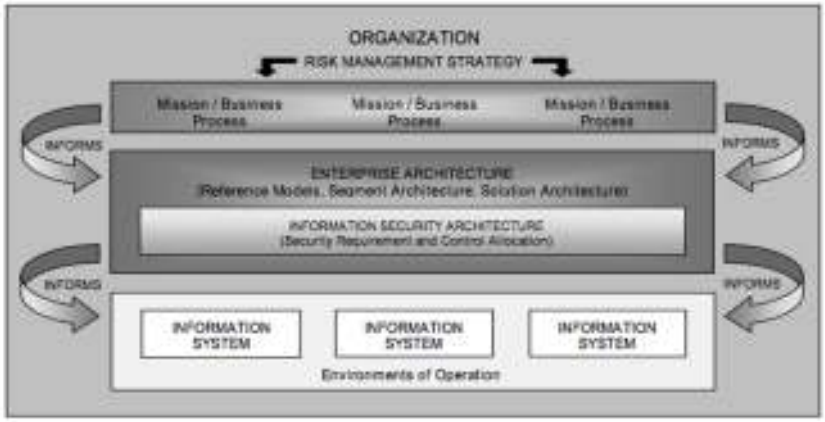
- Assigning risk management responsibilities to senior leaders/executives.
- Senior leadership's recognizing and understanding information security risks to organizational operations and assets, individuals, and other organizations.
- Establishing the organizational tolerance for risk and communicating the risk tolerance throughout the organization, including guidance on how risk tolerance impacts ongoing decision-making activities.
- Accountability by senior leadership for their risk management decisions and for the implementing of effective, organization-wide risk management programs.

5.1 Integration requirements

Figure 7 illustrates the role of an organization's risk-management strategy; it clearly identifies requirements for information security architecture at the enterprise level and information system at the operations level. These requirements are defined from top to bottom such that all layers are integrated and aligned with the organization's mission, business functions and processes. This type of strategy further ensures that the information security requirements are consistent, cost effective and efficient throughout the entire system. Ultimately, integrating information security into the organization's risk-management strategy will provide a clear and detailed roadmap that links the organization's strategic goals and objectives to specific information security solutions.

FIGURE 7

Integration of Information Security in Risk Management



Source: NIST SP 800

- The **enterprise architecture layer** is designed to provide a well-structured approach to consolidate, standardize and optimize transit agencies information technology assets. Information security risks can be reduced through integrating management processes throughout the entire agency, resulting in reinforced levels of security, privacy, reliability and cost savings. Integrating the organization's risk management strategy into the enterprise architecture layer will allow senior leadership to make more

informed decisions in a unique and dynamic environment—decisions based on trade-offs between fulfilling and improving organizational missions and business functions and managing the many types and sources of risk that must be considered in their risk-management responsibilities.

- The **information security architecture layer** is information system specific, including operational systems, systems under development and systems undergoing modification, as well as the system development life cycle. Risk management activities are also integrated into the system development life cycle of organizational information systems at this layer. The risk-management activities at the information security architecture layer are tied to the enterprise architecture layer and the strategic level to the organization's mission, business function and risk management strategy. Risk management activities take place at every phase in the system development life cycle, with the outputs at each phase having an effect on subsequent phases.

6. System contingency and resiliency

System resiliency is directly tied in with the transit agency's business continuity plan. It is essential for a transit agency, which thousands of customers are dependent on, to provide uninterrupted service as expected. Resiliency is the ability of a transit agency to mitigate disruptive services and quickly return to its original state after an incident. Transit agencies must identify and prioritize their vital services in all operating conditions through a thorough business impact analysis. Effective contingency planning includes incorporating security controls early in the development of an information system and maintaining these controls on an ongoing basis. By following a simple seven-step process as outlined in NIST 800-100, "Seven-Step IT Contingency Planning Process" (summarized in **Figure 8**), transit agencies will have the ability to quickly identify a security incident and take appropriate steps to recover from such an incident.

FIGURE 8
Integration of Information Security in Risk Management

Resilience, as defined by DHS, is the ability to quickly adapt and recover from any known or unknown changes to the environment. The goal of a resilient organization is to continue mission-essential functions at all times during any type of disruption. Resilient organizations continually work to adapt to changes and risks that can affect their ability to continue critical functions. Risk management, contingency and continuity planning are individual security and emergency management activities that can also be implemented in a holistic manner across an organization as components of a resiliency program.

6.1 Types of plans

Information system contingency planning represents a broad scope of activities designed to sustain and recover critical system services following an emergency event. Information system contingency planning fits into a much broader security and emergency management effort that includes organizational and business process continuity, disaster recovery planning and incident management. Ultimately, an organization would use a suite of plans to properly prepare response, recovery and continuity activities for disruptions affecting the organization's information systems, mission/business processes, personnel and facility. The following

plans support the organization's contingency and resiliency planning activities and should be considered in developing in an overall effort of creating a resilient organization against cybersecurity incidents:

- **Incident Response Plan:** This addresses the ability to proactively detect, contain, eradicate and recover from a security breach, such as from malware or an active network penetration leaking a transit agency's confidential information. The Federal Information Security Management Act (FISMA) specifically directs all federal agencies to develop and implement procedures for detecting, reporting and responding to security incidents. This practice will be useful and beneficial and for all transit agencies at the state and local level to consider. 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 while working with other agencies to foster a synergy of information sharing. All transit agencies should have some form of incident response.
- **Business Continuity Plan:** The BCP focuses on sustaining an organization's mission/business processes during and after a disruption. An example of a mission/business process may be an organization's payroll process or its customer service process. A BCP may be written for mission/business processes within a single business unit or may address the entire organization's processes. The BCP may also be scoped to address only the functions deemed to be priorities. A BCP may be used for long-term recovery in conjunction with the Continuity of Operations Plan, allowing for additional functions to come online as resources or time allow. 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:** The COOP focuses on restoring an organization's mission-essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. Additional functions, or those at a field office level, may be addressed by a BCP. Minor threats or disruptions that do not require relocation to an alternate site typically are not addressed in a COOP plan.
- **Crisis Communications Plan:** Organizations should document standard procedures for internal and external communications in the event of a disruption using a crisis communication plan. A crisis communications plan is often developed by the organization responsible for public outreach. The plan provides various formats for communications appropriate to the incident. The crisis communications plan typically designates specific individuals as the only authority for answering questions from or providing information to the public regarding emergency response. The plan may also include procedures for disseminating reports to personnel on the status of the incident and templates for public press releases.
- **Disaster Recovery Plan:** The DRP applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period. A DRP is an information system–focused plan designed to restore operability of the target system, application or computer facility infrastructure at an alternate site after an emergency. The DRP may be supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established. A DRP may support a BCP or a COOP by recovering supporting systems for mission/business processes or mission essential functions at an alternate location. The DRP addresses only information system disruptions that require relocation.

7. System and service acquisition

With fast-paced advancement of ICT technology, an organization capability of identifying, developing, implementing and retiring ICT equipment will be vital to achieve the most current and highest level of security protection. A critical function of a transit agency's IT security is the acquisition process. The acquisition process is not only about the procurement of information technology equipment to fulfill the direct immediate needs of the organization, but it also must encompass security throughout the whole process.

Every phase of procurement needs to meet and be vetted through a set of minimal security requirements defined by the agency and complying with any federal, state and local mandates.

The overall resiliency of a transit agency's information systems (i.e., how well systems operate while under stress) is a key factor and performance measure in determining the potential survivability of missions/business functions. The use of certain information technologies may introduce inherent vulnerabilities into these information systems, resulting in risk that may have to be mitigated by reengineering the current mission/business processes. The wise use of information technologies during the design, development and implementation of organizational information systems is of paramount importance in managing risk.

7.1 System Development Life Cycle

By utilizing the System Development Life Cycle (SDLC) process, transit agencies can more effectively manage their ICT systems. Many SDLC models have been developed, but they generally cover five major phases: initiation, development/acquisition, implementation, operations/maintenance and disposal. With the goal of maintaining information security through maintaining confidentiality, preserving integrity and sustaining availability, transit agencies must integrate security in each of the phases in the SDLC. Utilizing security activities outlined within each phase developed by NIST SP 800-100, transit agencies will have a broad understanding of the security activities necessary within the SDLC process. The following are the key security activities for each phase:

1. **Initiation**
    - Initial delineation of business requirements in terms of confidentiality, integrity and availability;
    - Determination of information categorization and identification of known special handling requirements to transmit, store or create information such as personally identifiable information; and
    - Determination of any privacy requirements.

2. **Development/acquisition**
    - Conduct the risk assessment and use the results to supplement the baseline security controls;
    - Analyze security requirements;
    - Perform functional and security testing;
    - Prepare initial documents for system certification and accreditation; and
    - Design security architecture.

3. **Implementation**
    - Integrate the information system into its environment;
    - Plan and conduct system certification activities in synchronization with testing of security controls;
    - Complete system accreditation activities.

4. **Operations/maintenance**
    - Conduct an operational readiness review;
    - Manage the configuration of the system;
    - Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls; and
    - Perform reauthorization as required.

5. **Disposal**
    - Build and execute a disposal/transition plan;
    - Archive critical information;
    - Sanitize media; and
    - Dispose of hardware and software.

7.2 Information security services and products

Information security services and products are essential elements of any organization's information security program. Many products and services to support an agency's information security program for information systems are widely available in the marketplace today.

Security products and services should be selected, used and integrated into a transit agency's information security program to manage, develop and maintain information security infrastructure, and to protect information. The acquisition process of security services and products should include risk management activities to identify and mitigate specific risks associated with such acquisition.

Transit agencies should weigh savings gained by outsourcing specific services against the risks connected to placing data and transactions outside of their own control and management. The importance of systematically managing the process for acquisition of information security services cannot be underestimated because of the potential impact associated with those risks.

Before selecting specific services, organizations should review the current status of their security programs and the security controls that are either planned or in place to protect information systems and data. Organizations should use the risk-management process to identify an effective mix of management, operational and technical security controls that will mitigate risk to an acceptable level. The number and type of appropriate security controls and their corresponding information security services may vary throughout a particular system's services life cycle.

8. Standards, resources and tools

APTA has identified industry standards, resources and tools for transit agencies to utilize and reference in developing specific information security programs tailored to individual agencies. These references are not exhaustive and are meant only to serve as a guide.

8.1 National Institute of Standards and Technology (NIST)

NIST is a non-regulatory U.S. federal agency responsible for developing standards and guidelines, including minimum requirements, and for providing adequate information security for all agency operations and assets. The SP 800 series provides guidance, description, details and standards in establishing and implementing information security programs. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.

Additionally, transit agencies should consider utilizing the Cyber Security Evaluation Tool (CSET®) from the Department of Homeland Security (DHS). It is a tool that assists organizations in protecting their key cyber assets. This tool provides users with a systematic and repeatable approach for assessing the security posture of their cyber systems and networks. It includes both high-level and detailed questions related to all industrial control and IT systems.

8.2 National Initiative for Cybersecurity Education (NICE)

The National Initiative for Cybersecurity Education (NICE) has evolved from the Comprehensive National Cybersecurity Initiative, and extends its scope beyond the federal workplace to include civilians and students in kindergarten through post-graduate school. The goal of NICE is to establish an operational, sustainable and continually improving cybersecurity education program encouraging sound cybersecurity practices that will enhance the nation's security. NICE will be represented by four components:

- **Component 1:** National Cybersecurity Awareness. Lead: DHS
- **Component 2:** Formal Cybersecurity Education. Co-Leads: Department of Education (DOE) and National Science Foundation (NSF)
- **Component 3:** Cybersecurity Workforce Structure. Lead: DHS supported by the Office of Personnel Management (OPM)
- **Component 4:** Cybersecurity Workforce Training and Professional Development. Tri-Leads: Department of Defense (DOD), Office of the Director of National Intelligence (ODNI), DHS.

8.3 International Organization for Standardization (ISO)

ISO is the world's largest developer of voluntary international standards. International standards give state-of-the-art specifications for products, services and good practice, helping to make industry more efficient and effective. Developed through global consensus, they help to break down barriers to international trade.

- ISO/IEC 13335: Information Technology Guidelines for the Management of IT Security
- ISO/IEC 17799: Code of Practice for Information Security Management
- ISO/IEC 27001: Information security management systems – Requirements
- ISO/IEC 27005: Information Security Risk Management
- ISO/IEC 31000: Risk Management Principles and Guidelines
- ISO/IEC 31010: Risk Management Risk Assessment Techniques
- ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation

8.4 APTA Cyber Standards & Guidance

The Control and Communications Cyber Security Work Group develops APTA standards for rail system control and communications security. The Control and Communications Security Work Group that began its work in 2007 published Part I of the APTA *Recommended Practice* "Securing Control and Communications Systems in Transit Environments" in 2010 (APTA-SS-CCS-RP-001-10). Part I is an introductory guide for transit agency cybersecurity and is focused on general principles such as describing transit system networks, organizing a cybersecurity program, and performing a cybersecurity risk assessment. Part I is limited in its cybersecurity scope and it does not address the specific use of cybersecurity technologies for prevention of attacks once cybersecurity risks are identified. Part II; (APTA-SS-CCS-RP-002-13) focuses on defining and applying security controls applied to high-risk/consequence and vital systems (safety-critical signaling systems, etc.) and medium risk/consequence systems (SCADA such as traction power systems, etc.), while laying out these security controls in the context of a transit agency security plan.

Additional guidance is available from "Ten Basic Cybersecurity Measures, Public Transportation Industry, Reducing Exploitable Weaknesses and Attacks in Communication and Control" which provides transportation cyber security officials, transportation agency general managers and other related stakeholder groups basic guidance and proactive steps for reducing vulnerability to a cyberattack. This document is available on HSIN-PT and on APTA's Safety & Security Resource page as an excellent resource for beginners and experts in cyber security.

8.5 Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act of 2002 is a U.S. federal law that recognizes the importance of information security to the economic and national security interests of the United States. FISMA has brought attention within the federal government to cybersecurity and emphasized a "risk-based policy for cost-effective security." FISMA requires agency program officials to conduct annual reviews of the agency's information security program and report the results to the Office of Management and Budget. The Office of Management and Budget uses this data to assist in its oversight responsibilities and to prepare this annual report to Congress on agency compliance with the act.

8.6 U.S. Computer Emergency Response Team (US-CERT)

The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation's cybersecurity posture, coordinate information sharing and proactively manage threats to the nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity: collaborative, agile and responsive in a dynamic and complex environment. US-CERT provides the following tools and resources:

- **National Vulnerability Database (NVD):** The NVD is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement and compliance.
- **Vulnerability Notes:** Vulnerability Notes contain information about vulnerabilities and include summaries, technical details, remediation information and lists of affected vendors.
- **Vulnerability Card Catalog:** Authorized users can log into the Vulnerability Card Catalog to access information regarding emerging vulnerabilities reported to the CERT Coordination Center.
- **US-CERT Portal:** The US-CERT Portal provides a secure, web-based, collaborative system to share sensitive, cybersecurity related information and news with participants in the public and private sector, including GFIRST, the CISO Forum, NCRCG, ISAC members, and various other working groups. Authorized users can visit the US-CERT Portal.
- **US-CERT Einstein Program:** This program provides an automated process for collecting, correlating, analyzing and sharing computer security information across the federal government to improve national situational awareness.
- **Security Configuration Benchmarks and Scoring Tools:** The Center for Internet Security (CIS) has security configuration benchmarks and scoring tools, many of which can be downloaded free of charge.
- **Build Security In:** A website that includes software assurance and software security information to help developers, architects, and security practitioners create secure systems.

8.7 Federal Information Processing Standard (FIPS)

A Federal Information Processing Standard (FIPS) is a publicly announced standardization developed by the U.S. federal government for use in computer systems by all non-military government agencies and by government contractors, when properly invoked and tailored on a contract. Many FIPS pronouncements are modified versions of standards used in the technical communities, such as the American National Standards Institute (ANSI), the Institute of Electrical and Electronics Engineers (IEEE), and the International Organization for Standardization (ISO).

8.8 SANS Institute

The SANS Institute was established as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. Ranges of individuals from auditors and network administrators to chief information security officers are sharing the lessons they learn and are jointly

finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.

References

Homeland Security, "Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise," November 2011. www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf

Executive Office of the President National Science and Technology Council, "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program," December 2011. www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

International Organization for Standardization, ISO/IEC 13335:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management

International Organization for Standardization, ISO/IEC TR 13335-3:1998, Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security outlines techniques and procedures to assist in IT security management and implementation.

International Organization for Standardization, ISO/IEC TR 13335-4:2000, Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards provides guidance on selecting safeguards that take into account organization-specific needs and concerns.

International Organization for Standardization, ISO/IEC TR 13335-5:2001, Information technology – Guidelines for the management of IT Security – Part 5: Management guidance on network security helps to identify and analyze communications-related factors when establishing network security requirements.

International Organization for Standardization, ISO/IEC 17799, Information technology – Code of Practice for Information Security Management.

International Organization for Standardization, ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements, is a certification standard intended to be used with ISO/IEC 17799.

National Institute of Standards and Technology, Special Publication 800 Series.
http://csrc.nist.gov/publications/PubsSPs.html:
- SP 800-30, "Risk Management Guide for Information Technology Systems," July 2002.
- SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," May 2004.
- SP 800-64, "Security Considerations in the Information System Development Life Cycle," October 2003.
- SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems," February 2006.
- SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 2010.
- SP 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View," March 2011.
- SP 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009.
- SP 800-53A, Revision 1, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans," June 2010.
- SP 800-59, "Guideline for Identifying an Information System as a National Security System," August 2003.

SP 800-60, Revision 1, "Guide for Mapping Types of Information and Information Systems to Security Categories," August 2008.
SP 800-39, "Managing Risk from Information Systems: An Organizational Perspective," April 2008.
SP 800-70, Revision 2, "National Checklist Program for IT Products – Guidelines for Checklist Users and Developers," February 2011.
SP 800-137 (Initial Public Draft), "Information Security Continuous Monitoring for Federal Information Systems and Organizations," December 2010.
SP 800-55, "Security Metrics Guide for Information Technology Systems," July 2003.

NIST Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004.

NIST Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006.

NIST ITL Bulletin: Selecting Information Technology Security Products, April 2004. http://csrc.nist.gov/publications/nistbul/04-2004.pdf

NIST ITL Bulletin: "Information Technology Security Services; How to Select, Implement, and Manage," June 2004. http://csrc.nist.gov/publications/nistbul/b-06-04.pdf

SANS Institute, "8 Simple Rules for Securing your Internal Network," September 2003. www.sans.org/reading_room/whitepapers/bestprac/8-simple-rules-securing-internal-network_1254

SANS Institute, "The Internal Threat to Security Or Users Can Really Mess Things Up," September 2003. www.sans.org/reading_room/whitepapers/bestprac/internal-threat-security-users-mess-things_856

SANS Institute, "Federal Information Technology Management and Security," September 2003. www.sans.org/reading_room/whitepapers/bestprac/federal-information-technology-management-security_1190

SANS Institute, "A Guide to Government Security Mandates," December 2002. www.sans.org/reading_room/whitepapers/bestprac/guide-government-security-mandates_1000

US-CERT, "Recovering from a Trojan Horse or Virus," 2008. www.us-cert.gov/reading_room/trojan-recovery.pdf

US-CERT, "Introduction to Information Security," 2008. www.us-cert.gov/reading_room/infosecuritybasics.pdf

US-CERT, Technical Information Paper-TIP-11-075-01, "System Integrity Best Practices," March 2011. http://cryptome.org/0003/rsa-apt-wand.pdf

U.S. Department of Transportation, Enterprise Architecture and Business Transformation Office, "Enterprise Transition Plan," June 2009. www.dot.gov/cio/docs/ETS_FY2009.pdf

U.S. Government Accountability Office (GAO), "National Cybersecurity Strategy: Key Improvements are Needed to Strengthen the Nation's Posture," testimony before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives, March 2009. www.gao.gov/new.items/d09432t.pdf

Definitions

Enterprise Cybersecurity Is the body of technologies, processes and practices designed to protect business and IT networks, computers, programs and data from threats, attacks, damage or unauthorized access.

Information security (INFOSEC) Information is an asset to all individuals and businesses. Information Security refers to the protection of these assets in order to achieve confidentiality - Integrity - Availability

Intrusion Detection Monitoring network or system activities for unauthorized or malicious activities or policy violations.

Secure Cloud Cloud computing security refers to the set of procedures, processes and standards designed to provide information security assurance in a cloud computing environment.

System Penetration Penetration testing (pen-testing or pentesting) is a method of testing, measuring and enhancing established security measures on information systems and support areas. Pen-testing is part of the overall IT security assessment.

Abbreviations and acronyms

APTA	American Public Transportation Association
ANSI	American National Standards Institute
BCP	Business Continuity Plan
CIS	Center for Internet Security
CISO	chief information security officer
CIO	chief information officer
COOP	Continuity of Operations Plan
CRM	customer relationship management
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Education
DOT	Department of Transportation
DRP	Disaster Recovery Plan
EIS	enterprise information system
ERP	enterprise resource planning
FIPS	Federal Information Processing Standard
GAO	Government Accountability Office
FISMA	Federal Information Security Management Act
GFIRST	Government Forum of Incident Response and Security Teams
GUI	graphical user interface
HIPAA	Health Insurance Portability and Accountability Act
HVAC	heating, ventilation, air conditioning
ICT	information and communication technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INFOSEC	information security
IR	infrared
ISAC	Information Sharing & Analysis Center

ISP	Internet service provider
IT	information technology
ITL	Information Technology Laboratory (NIST)
KMS	knowledge management system
ISO	International Organization for Standardization
NCRCG	National Cyber Response Coordination Group
NSF	National Science Foundation
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
ODNI	Office of the Director of National Intelligence
OEM	original equipment manufacturer
OPM	Office of Personnel Management
PCI	payment card industry
SANS	SysAdmin, Audit, Networking and Security
SDLC	system development life cycle
SCADA	supervisory control and data acquisition
SCAP	Security Content Automation Protocol
SCM	supply chain management
SDLC	System Development Life Cycle
SSL	secure socket layer
SP	(NIST) Special Publication
TI	transportation information
TSA	Transportation Security Administration
US-CERT	United States Computer Emergency Readiness Team