Roadmap to Secure Control Systems in the Transportation Sector





August 2012

prepared by

The Roadmap to Secure Control Systems in the Transportation Sector Working Group

VERSION CONTROL SHEET

Version	Date
1.0	May 31, 2012
2.0	July 20, 2012
3.0	August 31, 2012

FOREWORD

The Roadmap to Secure Control Systems in the Transportation Sector (Transportation Roadmap) describes a plan for voluntarily improving industrial control systems (ICSs) cybersecurity across all transportation modes: aviation, highway, maritime, pipeline, and surface transportation. This Transportation Roadmap provides an opportunity for transportation industry experts to offer input concerning the state of control systems cybersecurity and to communicate recommended strategies for improvement. This Transportation Roadmap brings together transportation stakeholders from all modes, including government agencies and asset owners and operators, by offering a common set of cybersecurity goals and objectives, with associated metrics and milestones for measuring performance and improvement over a ten-year period.

The U.S. Department of Homeland Security's (DHS's) National Cybersecurity Division (NCSD), Control Systems Security Program (CSSP) facilitated the development of this Transportation Roadmap, with volunteers from the transportation community. This Transportation Roadmap provides a beginning point and a template for action as industry and government work together to achieve a common objective of securing ICSs in the Transportation Sector.

Individual ICSs may have inherently different levels of cybersecurity due to modal differences, organizations'[1] business operations, specific policies followed, etc. Under some circumstances, an organization may decide not to activate an ICS cybersecurity feature, based on the organization's risk management assessment/plan, security considerations, or other reasons. Because transportation modes, as well as individual companies within each mode, are at different stages of identifying and implementing cybersecurity features, a "one size fits all" approach does not work for addressing cybersecurity in the Transportation Sector. The information presented in this Transportation Roadmap provides individual modes and companies with a logical continuum of activities and benchmarks they can use to identify the cybersecurity features currently in place and to determine the next activities for consideration to improve cybersecurity performance.

While the activities presented in this Transportation Roadmap are voluntary, they should be conducted in accordance with applicable laws and policies. Nothing in this Transportation Roadmap should be taken to restrict, supersede, or otherwise replace the legal authorities or regulatory responsibilities of any government agency or organization. The views expressed within this Transportation Roadmap are those of the members of the Transportation Roadmap Working Group and do not constitute an official agency or organization position.

[1] The term "organization" is used in this document to denote any public or private entity or company involved with transportation who is pursuing ICS cybersecurity improvement.

ROADMAP TO SECURE CONTROL SYSTEMS IN THE TRANSPORTATION SECTOR WORKING GROUP

Name		Organization/Company	Role
Jeffrey	Berenson	Department of Transportation	Member
Gene	Brooks	Maersk Line, Limited	Member
George	Cummings	Port of Los Angeles	Member
Kevin	Dow	American Public Transportation Association	Member
Brian	Fitzgibbon	Maersk Line, Limited	Member
Edward	Fok	Federal Highway Administration	Member
Alan	Greenberg	Boeing (formerly)	Member
Candace	Hancock	Maersk Line, Limited	Member
Kevin	Harnett	Department of Transportation	Member
Fred	Hellwig	Surface Transportation and Public Transportation Information Sharing and Analysis Centers	Member
Herasmo	Iñiguez	California Department of Transportation	Member
Dawn	Johnson	Department of Transportation	Facilitator
Lisa	Kaiser	Department of Homeland Security	ICSJWG Lead
Joshua	Poster	Surface Transportation and Public Transportation Information Sharing and Analysis Centers	Member
David	Sawin	Department of Transportation	Member
Peter	Sindt	Department of Homeland Security	Member
Janet	St. John	Surface Transportation Information Sharing and Analysis Center	Member
Chuck	Weissman	Los Angeles Metro	Member

Table of Contents

1.0 Introduction

Leaders from the nation's critical infrastructure and key resources (CIKR) sectors and government agencies recognize the need to plan, coordinate, and focus ongoing efforts to improve control system security. Industry stakeholders agree that a concise plan, with specific goals and milestones for implementing security across individual sectors, is required to prioritize critical needs and gaps to assist CIKR asset owners in reducing the risk of future cyber attacks on control systems.

In recent years, Energy, Water, Chemical, and other sector Roadmaps have been developed to guide the efforts of individual sectors in securing their industrial control systems (ICSs). In addition, a Cross-Sector Roadmap, designed to address cybersecurity issues related specifically to ICSs owned and operated by agencies and industries whose facilities are part of the nation's CIKR, was finalized in 2011 through the Industrial Control Systems Joint Working Group (ICSJWG). Roadmaps develop near, mid, and long-term perspectives (typically over a ten-year period) to guide industry efforts toward common high-level goals. Roadmaps provide an opportunity for industry experts and sector stakeholders to evaluate the state of their sector's ICSs cybersecurity, to identify and resolve gaps in protective measures, and to identify appropriate strategies for securing ICSs in their sector; together, these activities provide a consistent approach for reducing risks so that stakeholders can implement the high-level goals identified in the sector-specific plan.

ICSs are 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, then relay control commands to local or remote equipment or to human-machine interfaces (operators).

Definition modified from DHS, *National Cyber Security Division Style Guide*, February 2012, page 40, and Water Sector Coordinating Council Cyber Security Working Group, *Roadmap to Secure Control Systems in the Water Sector*, March 2008, page 11.

This Transportation Roadmap presents broad descriptions of ICSs[2] in each mode of the Transportation Sector, associated ICSs cybersecurity risks and challenges, and general methods for improving the cybersecurity of transportation ICSs over the next decade. Implementation of the information presented in this Roadmap is voluntary, and each organization has the flexibility to review, evaluate, and apply the ideas and concepts presented herein within the context of its overall cybersecurity program, policies, and procedures.

Transportation Sector ICSs

ICSs in the Transportation Sector include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), programmable logic controllers (PLCs), and general-purpose controllers (GPCs). The scope of facilities and equipment encompassed by these technologies range from broadly dispersed operations, such as natural gas pipelines and water distribution systems, to individual machines and processes.

Most ICSs began as proprietary, stand-alone systems that were separated from the rest of the world and isolated from most external threats. Today, widely available software applications, Internet -enabled devices and other nonproprietary information technology (IT) offerings have been integrated into most ICSs. This connectivity has delivered many benefits, but it also has increased the vulnerability of these systems to malicious attacks, equipment failures, and other threats.

As a rule, ICSs must operate continuously and reliably, often around the clock. Unlike IT systems (which process, store, and transmit digital data), ICSs typically monitor the system environment and control physical objects and devices, such as switchgears, message signs, and valves; these devices are often located in remote locations. ICS disruptions or failures can result in death or injury, property damage, and loss of critical services.

Sources: NIST website at URL www.nist.gov/el/isd/ics-062111.cfm and Wikipedia

[2] In the document, the term "ICSs" includes all process control systems, functional and operational systems, safety systems tied to operational systems, supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), programmable logic controllers (PLCs), and general-purpose process controllers. It does not include business systems and information technology (IT) systems.

2.0 Purpose

This Transportation Roadmap serves as a tool for transportation entities to improve the security of their ICSs. This Transportation Roadmap is intended to be used as a guide for transportation entities within each mode to determine their current cybersecurity posture, identify near, mid, and long-term objectives necessary to better secure ICSs, and evaluate their progress towards better securing their ICSs from cyber risks and threats. This Transportation Roadmap:

> *"Several sectors are developing Roadmaps that establish a vision for securing control systems within the sector, and include goals, objectives, measures, and timetables to meet the vision. Roadmaps develop a near, mid, and long-term perspective to guide industry efforts toward a common goal. Those created so far are detailed enough to enable stakeholders to evaluate their security posture, identify and resolve gaps in protective measures, and provide a consistent approach for reducing risks so that stakeholders can implement the high level goals identified in the sector-specific plan."*
>
> DHS, *Strategy for Securing Control Systems*, October 2009

- Defines a consensus-based strategy that addresses the specific cybersecurity needs of transportation asset owners and operators,
- Proposes a comprehensive plan for improving the security, reliability, functionality, and oversight of transportation ICSs,
- Proposes methods and activities that encourage participation and compliance by all stakeholders,
- Guides modal cybersecurity efforts, and
- Presents a vision—along with a supporting framework of goals, objectives, and milestones and metrics—for continuous improvement of the cybersecurity of ICSs in the Transportation Sector.

3.0 Scope

This Transportation Roadmap presents general cybersecurity information applicable to modal ICSs in the Transportation Sector. Other transportation operating and maintenance systems are not included in the scope of this document.

Careful evaluation and analysis of all risk factors—including physical, cyber, and human—need to be considered when designing, operating, and maintaining transportation facilities, processes, and equipment. While attacks on a cyber system may involve only the cyber components and their operation, those impacts can extend into the physical, business, human, and environmental systems to which they are connected. A cyber event, whether caused by an external adversary, an insider, or inadequate policies and procedures, can initiate a loss of system control, resulting in negative consequences. This Transportation Roadmap recognizes these interconnectivities, but restricts its scope by addressing only the cyber issues of ICSs.

Securing access to and control of the business network and Internet is generally the responsibility of information technology (IT) personnel, and thus outside the scope of this Transportation Roadmap. Similarly, physical access to cyber systems is a significant contributing factor of cyber risk, and physical damage resulting from cyber compromise is one of the principal factors contributing to industrial control systems risk. While this Transportation Roadmap includes both of these factors in understanding and planning for cybersecurity enhancements, actual engagement in physical access control and physical consequence management outside of physically securing cyber assets is beyond the scope of this Transportation Roadmap.

This Transportation Roadmap covers goals, objectives, and metrics and milestones over the near (0–2 years), mid (2–5 years), and long (5-10 years) terms. Security needs encompass research and development (R&D), new technologies, systems testing, training and education, accepted industry practices, standards and protocols, policies, information sharing, and outreach and implementation.

While the general cybersecurity information presented in this document are applicable to most transportation ICSs, the National Airspace System (NAS) governed by the Federal Aviation Administration (FAA) is not covered by this Transportation Roadmap because the FAA already has a mature cybersecurity program in place. As the Transportation Roadmap matures, the transportation community should collaborate with the NAS's cybersecurity program to gain and share lessons learned.

4.0 National Context

The Homeland Security Presidential Directive (HSPD) 7, *Critical Infrastructure Identification, Prioritization, and Protection,* required the National Infrastructure Protection Plan (NIPP) to provide the collaborative framework and unifying structure for the integration of existing and future CIKR protection efforts for the government and private sector. These collaborative partnerships consist of a Sector Coordinating Council (SCC) and a Government Coordinating Council (GCC.)

HSPD-7 also assigned Sector-Specific Agencies (SSAs) for each of the 18 CIKR sectors. SSAs are the lead agencies responsible for collaborating with other Federal, State, local, tribal, territorial, and private sector partners. The SSAs are responsible for implementing and encouraging the development of information sharing and analysis mechanisms, including the sharing of information regarding physical and cyber threats, vulnerabilities, incidents, potential protective measures, and accepted industry practices. The NIPP requires sectors to issue sector-specific plans that address security posture and initiatives to achieve security. The Transportation Security Administration (TSA) is the SSA for the Transportation Systems Sector, and the U.S. Coast Guard (USCG) is the SSA for the Maritime Mode.[3]

[3] DHS, *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan*, 2010, Section 1.2.1.

In 2004, the Department of Homeland Security's (DHS'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 2009, the CSSP also established the 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.

Appendix A summarizes national policy guidance on cybersecurity of industrial control systems.

5.0 Action Plan

This Transportation Roadmap presents the first iteration of a voluntary strategic framework for industry and government to address ICSs cybersecurity in the Transportation Sector. As an action plan, the Transportation Roadmap is designed to improve the Transportation Sector's resiliency against cyber events that would disrupt transportation operations and have negative consequences. This document describes activities that should be addressed, presents cybersecurity challenges, and outlines specific metrics and milestones to be accomplished over the next ten years to achieve the identified cybersecurity goals and objectives. While this Transportation Roadmap contains many actionable items, it is only useful to the extent that modal industries and government organizations[4] dedicate the financial resources, intellectual capability, commitment, and leadership necessary for translating these goals, objectives, and metrics and milestones into productive projects, activities, and products within their respective organizations.

Appendix B describes the process the Transportation Roadmap Working Group followed during the development of this document.

[4] The term "organization" is used in this document to denote any public or private entity or company involved with transportation who is pursuing ICS cybersecurity improvement.

6.0 Control Systems in the Transportation Landscape

6.1 General Overview of ICSs

"ICS" is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), programmable logic controllers (PLCs), and general purpose controllers (GPCs). ICSs perform various functions and exist at different stages of evolution throughout the nation's CIKR. Many of the ICSs used today were designed for availability and reliability during an era when security received low priority. These systems operated in fairly isolated environments and typically relied on proprietary software, hardware, and communications technologies. Infiltrating and compromising these systems often required specific knowledge of individual system architectures and physical access to system components. An illustration of the basic operation of an ICS is shown in Figure 1.

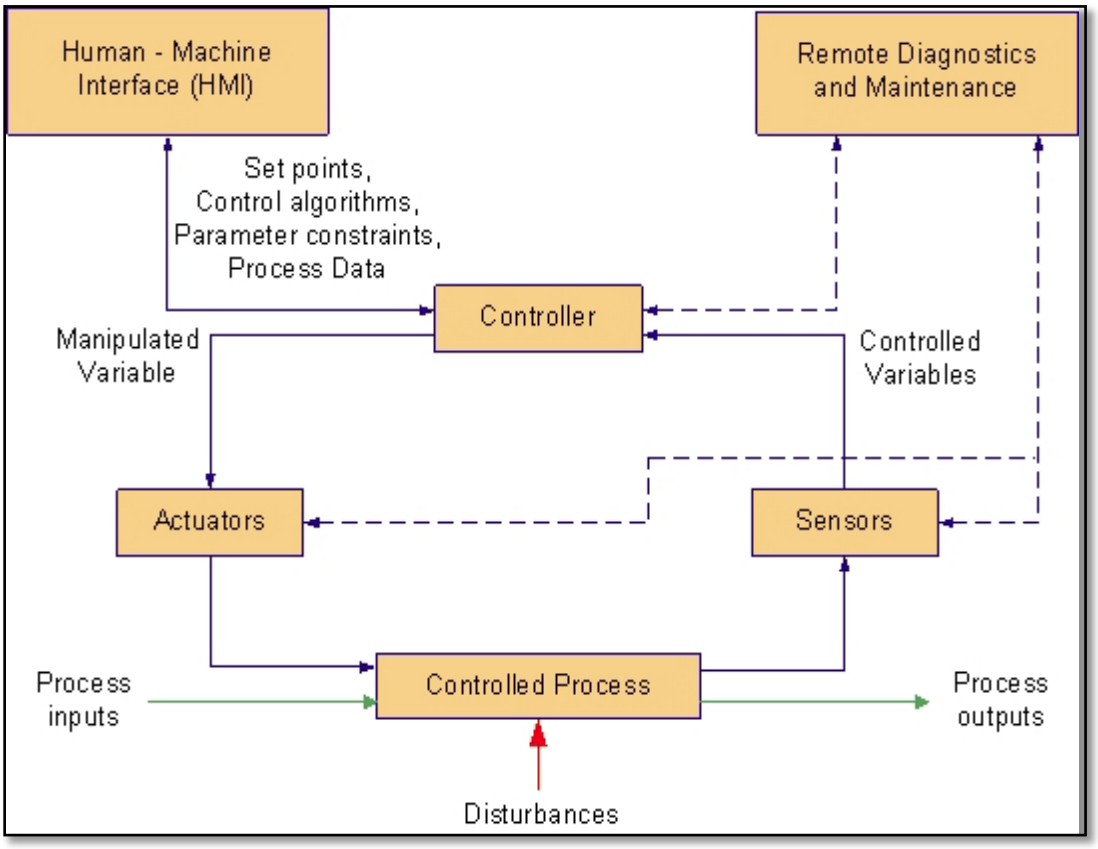

Figure 1: ICS Operation[5]

6.1.1 SCADA Systems

SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometers, where centralized data acquisition and control are critical to system operation. They are used in distribution systems such as oil and

[5] Source: NIST Special Publication 800-82, *Guide to Industrial Control Systems Security*, page 2-3, June 2011.

natural gas pipelines and in railway transportation systems. SCADA systems are also used to control all operational aspects, including remote operation, of ship-to-shore and rail-mounted gantry cranes at marine ports and terminals. A SCADA control center performs centralized monitoring and control for field sites over long-distance communications networks, including monitoring alarms and processing status data. Based on information received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices, which are often referred to as field devices. Field devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, directing automated train routings, monitoring local environments for alarm conditions, and monitoring of automated identification systems.

6.1.2 DCSs

DCSs are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated sub-systems that are responsible for controlling the details of a localized process. Product and process control are usually achieved by deploying feedback or feed forward control loops whereby key product and/or process conditions are automatically maintained around a desired set point. While DCSs are used extensively in process-based industries, Central traffic management systems are examples of DCSs used in transportation.

6.1.3 PLCs

PLCs are computer processor-based solid-state devices that control industrial equipment and processes. PLCs are used in transportation to control operational activities associated with systems and equipment such as airport baggage systems; heating, ventilation, and air conditioning (HVAC) systems; port cranes used to load and unload cargo from ships; and access gates. PLCs are also used extensively in transportation to implement safety and interlocking functions that, if compromised, could pose an immediate threat to life and property.

6.1.4 GPCs

GPCs are industrial computers that control and meter vehicular flow in freeways and arterials. They typically operate in standalone, direct, and/or distributed mode.

- In “standalone” control mode, the GPC is operating independently in the field without external communication. The GPC exercises control using locally stored schedules, predefined control algorithms, or via manual operation by a person at the GPC. Device monitoring might include processing of local sensor information and/or monitoring the results of the controller’s control actions. Interactions with the GPC take place through the device's integral interface, laptop interfaces, or similar portable device.
- For “direct” control mode, commands are sent from a control center or a master GPC over a communications network to affect the operation of local or slave GPCs.
- The “distributed” control mode is a combination of the first two. Here the local GPCs exercises normal control but the operation is managed and synchronized with a central management system or master GPC. Local control may be overridden remotely by the management system to meet wide area needs.

Key ICS components include:

- ***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.
- ***Human-Machine Interface (HMI)*.** Operators and engineers use HMIs to monitor and configure set points, control algorithms, and adjust and establish parameters in the controller. The HMI also displays process status information and historical information.
- ***Remote Diagnostics and Maintenance Utilities*.** In addition to general maintenance and configuration management, diagnostics and maintenance utilities are used to prevent, identify, and recover from abnormal operation or failures.

A typical ICS contains a proliferation of control loops, HMIs, and remote diagnostics and maintenance tools built using an array of network protocols on layered network architectures. Sometimes these control loops are nested and/or cascading, whereby the set point for one loop is based on the process variable determined by another loop.

In contrast, newer ICSs are highly network-based and use common standards for communication protocols. Many controllers are Internet Protocol (IP) addressable. Asset owners and operators have gained immediate benefits by extending the connectivity of their ICS, and have increasingly adopted commercial off-the-shelf (COTS) technologies that provide the greater levels of interoperability required among today's modern infrastructures. Today's ICSs, critical to the operation of the U.S.'s CIKR sectors, are often highly interconnected and mutually dependent systems. Standard operating systems such as Windows, UNIX, or Linux are increasingly used in ICSs, which are now typically connected to remote controllers via private networks provided by telecommunications companies. Common telecommunications technologies such as the Internet, public-switched telephone, cable, or wireless networks are often used. Figure 2 depicts the components and general configuration of a typical SCADA system.

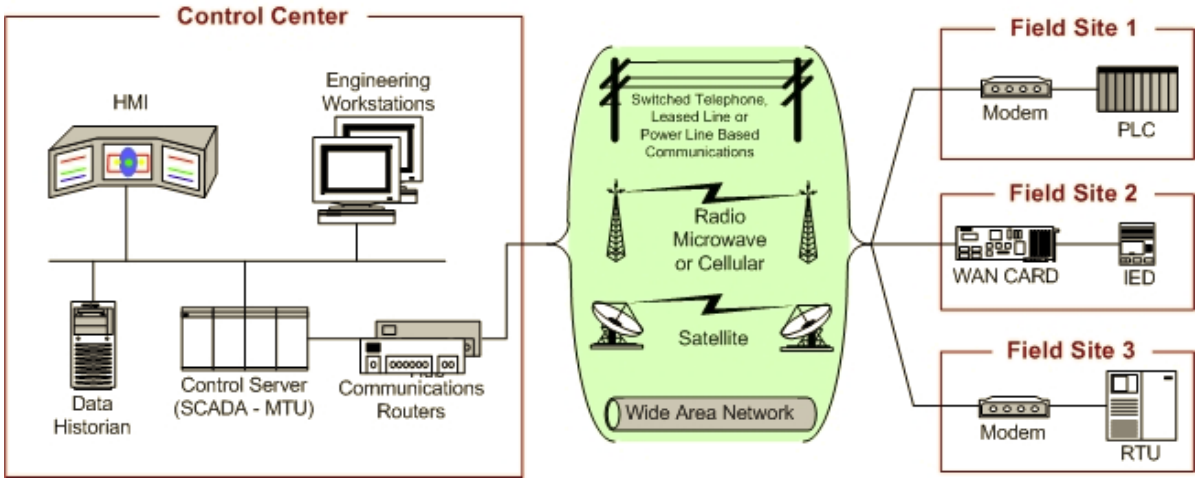

Figure 2: SCADA System General Layout[6]

The potential for system access resulting from this interoperability exposes network assets to infiltration and subsequent manipulation of sensitive operations. Furthermore, increasingly sophisticated cyber attack tools can exploit vulnerabilities in COTS system components, telecommunication methods, and common operating systems found in modern control systems. The ability of asset owners to discover and understand such emerging threats and system vulnerabilities is a prerequisite to developing effective security polices and countermeasures.

The incorporation of IT components into ICSs can render such ICSs vulnerable to viruses and attack methods traditionally associated with IT systems. In addition, modern IT networks often place higher priority on the security of data confidentiality and integrity than on data availability, while most ICSs security priorities are the opposite (because of the need for high availability of valid data).[7]

Even though ICSs are designed for reliability, ICS security policies and practices are often poorly implemented. As operating practices have evolved to allow real-time operation and control of critical assets, protecting ICSs from cyber risks has become more difficult. The following descriptions provide information on some of the most serious security issues, and associated challenges, inherent in current ICSs.

Increased Connectivity. Today's ICSs are being increasingly connected to company enterprise systems that rely on common operating platforms and are accessible through the Internet. Even though these changes improve operability, they also create serious vulnerabilities because improvements in the security features of control systems are not concurrent.

Interdependencies. Due to the high degree of interdependency among infrastructure sectors and transportation modes, failures within one sector/mode can spread into others. A successful cyber attack might be able to take advantage of these interdependencies to produce cascading impacts and amplify the overall economic damage.

---

[6] Source: NIST Special Publication 800-82, *Guide to Industrial Control Systems Security*, page 2-7, June 2011.
[7] DHS, *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth-Strategies*, October 2009, Section 2.

Complexity. The demand for real-time information-sharing and control has increased system complexity in several ways: access to ICSs is being granted to more users, business and control systems are interconnected, and the degree of interdependency among infrastructures has increased. Dramatic differences in the training and concerns of those in charge of IT systems and those responsible for control system operations have led to challenges in coordinating network security between these two key groups.

Legacy Systems. Although older legacy ICSs may operate in more independent modes, they tend to have inadequate password policies and security administration, no data protection mechanisms, and protocols that are prone to snooping, interruption, and interception. These insecure legacy systems have long service lives and will remain vulnerable for years to come unless these problems are mitigated.

System Access. Even limited connection to the Internet exposes control systems to all of the inherent vulnerabilities of interconnected computer networks, including viruses, worms, hackers, and terrorists. Control channels that use wireless or leased lines that pass through commercial telecommunications facilities may also provide minimal protection against forgery of data or control messages. These issues are of particular concern in industries that rely on interconnected enterprise and control networks with remote access from within or outside the company.

Offshore Reliance. Many software, hardware, and control system manufacturers are under foreign ownership or develop systems in countries whose interests do not always align with those of the U.S. Also of concern is the practice of contracting ICS's support, service, and maintenance to third parties located in foreign countries.

Information Availability. ICSs manuals and training videos are publicly available and many hacker tools can now be downloaded from the Internet and applied with limited system knowledge. Attackers do not have to be experts in control operations to access ICSs.

Configuration Management/Maintenance. Some transportation systems can be accessed by external users via networks, devices, and software components either directly (i.e., wired access) or remotely (i.e., wireless) for scheduled or corrective maintenance purposes. Examples of such systems include aircraft avionics, traffic management systems, and railway positive controls systems. Potential security vulnerabilities arise from access by unauthorized users and for corruption of resources (e.g. applications, databases, configuration files, etc.), whether intended or by accident.

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.us-cert.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."[8]

[8] Refer to Appendix D: References.

6.2 Aviation Mode

The Aviation Mode is composed of aircraft, air traffic control systems, approximately 450 U.S. commercial airports, and about 19,000 public airfields. Included in this mode are civil and joint-use military airports, heliports, short takeoff and landing airports, and seaplane bases.[9]

The U.S. NAS, governed by the FAA, consists of a ground-based air traffic control system that directs aircraft traffic on the ground and in the air. While much of the information contained in the document may apply to the NAS, the NAS already has a mature cybersecurity program in place; for this reason, this Roadmap focuses on other aviation electronic control systems used to operate airlines and entertain aircraft passengers; namely, control systems associated with airline information services and passenger information and entertainment services. In addition, while some of the newer avionics control systems may fit in more than one category, and some of their functionality crosses into one or more subcategories.

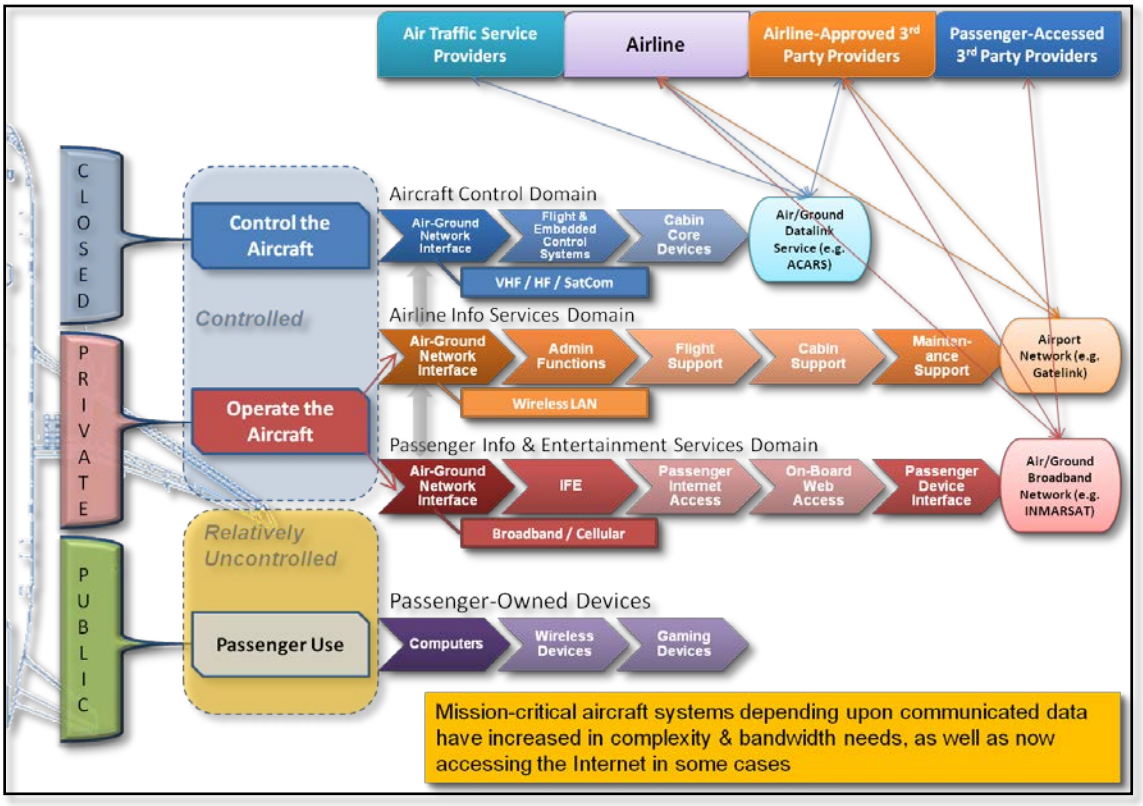

Figure 3: Aircraft Information Domains and Interconnections[10]

[9] DHS, *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010, Table 1-1.

[10] Figure 3 was created from information derived from Aeronautical Radio, Inc.'s, *Draft 2-ARINC Project Paper 811, Commercial Aircraft Information Security, Concepts of Operation and Process Framework*, Figure, 2, July 22, 2005.

New generation electronic-enabled (e-enabled) aircraft (such as the Boeing 787, Airbus A380, Airbus A350, Bombardier CSeries, Gulfstream 650, and others) and retrofitted legacy aircraft implement an unprecedented amount of new technologies such as IP-enabled networks, COTS, wireless connectivity (e.g., Bluetooth®), and global positioning systems (GPSs). Aircraft/avionics manufacturers are implementing "wireless" systems to reduce the amount of wiring within an aircraft. The reduction in weight helps an aircraft achieve lower fuel consumption and can also reduce support costs by simplifying aircraft configurations; however, these wireless systems are vulnerable to cybersecurity threats.

With the introduction of new generation e-enabled aircraft, a new era has begun where aircraft navigation and communication functions are transitioning from operating as isolated and independent system to being integrated into a centralized network system that is dependent on exchanging digital information between the e-enabled aircraft and external networks located on the ground and on other e-e-enabled aircraft. Current aircraft systems architectures are relying heavily on IP-based networks that interconnect aircraft systems such as flight controls, displays, avionics, engine, and cabin systems. While providing unprecedented global connectivity, these e-enabled aircraft technologies and COTS components introduce many access points to aircraft networks; as a result, e-enabled security vulnerabilities not present in past aircraft designs have the potential to significantly impact current aircraft safety.

At the same time, unprecedented access to aircraft systems and networks from external systems—including GateLink, wireless local area networks (WLANs), Avionics Full Duplex Switched Ethernet (AFDX) Networking, engine health and usage monitoring systems (HUMSs), and electronic flight bags (EFBs)—are being introduced. While

External Systems

GateLink is a system that employs WLAN technology to transmit data from a docked aircraft to destinations throughout an airport. The data can be shared between aircraft and passenger terminals, maintenance operations, baggage handling, ground support, and other airport operations. (Source: *Aviation Today*, "Wireless GateLink: Coming of Age," July 1, 2005. URL is available at: www.aviationtoday.com/av/issue/feature/Wireless-GateLink-Coming-of-Age_996.html)

A WLAN links two or more devices using some wireless distribution method and usually providing a connection through an access point to the wider internet. These features give users the mobility to move around within a local coverage area and still be connected to the network. Most modern WLANs are based on IEEE 802.11 standards. (Source: Wikipedia)

AFDX is a data network for safety-critical applications that utilizes dedicated bandwidth while providing deterministic quality of service. AFDX is based on IEEE 802.3 Ethernet technology and utilizes COTS components. (Source: Wikipedia)

HUMS is a generic term given to activities that utilize data collection and analysis techniques to help ensure availability, reliability and safety of vehicles, particularly rotary wing aircraft. (Source: Wikipedia)

EFB is an electronic information management device designed to help flight crews perform flight management tasks more easily and efficiently with less paper by providing a general purpose computing platform for reducing/replacing paper-based reference materials traditionally stored in the pilot's carry-on flight bag. The EFB can also host purpose-built software applications to automate other functions normally conducted by hand, such as performance take-off calculations. (Source: Wikipedia)

these connections allow for the convenience of two-way transfer of critical information to and from the airplane, this two-way information transfer makes it easier for inaccurate information to be transferred—either by mistake or through malicious intent—to and from the airplane.

6.3 Highway Mode

The U.S. Highway Mode includes more than four million miles of interstate highway, strategic highways, arterial roadways, intermodal connectors and their associated infrastructure, such as bridges and tunnels. This network of roadways provides access to various transportation vehicles, including automobiles, school buses, motorcycles, and all types of trucks, trailers, and recreational vehicles.[11]

The nation's roadway infrastructure is interconnected not just with asphalt and concrete, but by control systems which ensure the infrastructure's safe operation for motorists. These interconnected road networks are controlled by numerous systems composed of traffic signal controllers, ramp meters, dynamic message signs, roadway sensors, road weather information sensors, etc. These devices are frequently connected into a traffic management center where roadway operators monitor both traffic conditions and the status of the control systems to ensure safe and efficient transportation.

For the last 20 years, the highway industry has embraced Intelligent Transportation Systems (ITS) to improve performance in both operational efficiencies and roadway mobility. ITS leverages advances in communication and computer technologies to maximize safety, mobility, and environmental performance.

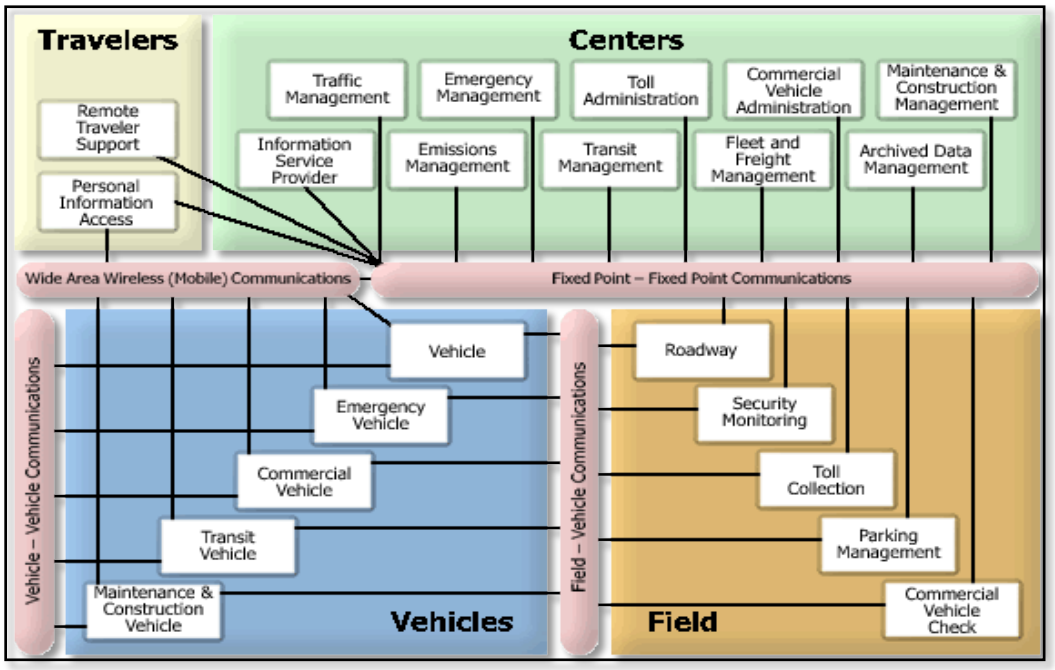

Figure 4: Highway/Roadway Network System[12]

[11] DHS, *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010, Table 1-1.

[12] Source: "National ITS Architecture Subsystems and Communications," courtesy of the Federal Transit Administration.

Figure 4 displays the 22 possible types of ITS subsystems; the two most prevalent are the traffic management and roadway subsystems. In most large metropolitan areas, the traffic management center is part of a transportation management system that links control systems from multiple agencies and multiple modes together to improve coordination. These control systems use information from traffic sensors, such as loop detectors, to regulate the flow of traffic entering roadways and freeways by monitoring traffic flow and signaling traffic light changes based on current traffic conditions. In addition, video surveillance systems are often used in tandem with signal systems to provide enhanced situational awareness to the operation staff and public information. Finally, applications such as signal preemption for emergency vehicles and signal priority for transit buses (used in advanced transit systems) are often integrated into the control systems and managed by the transportation management centers.

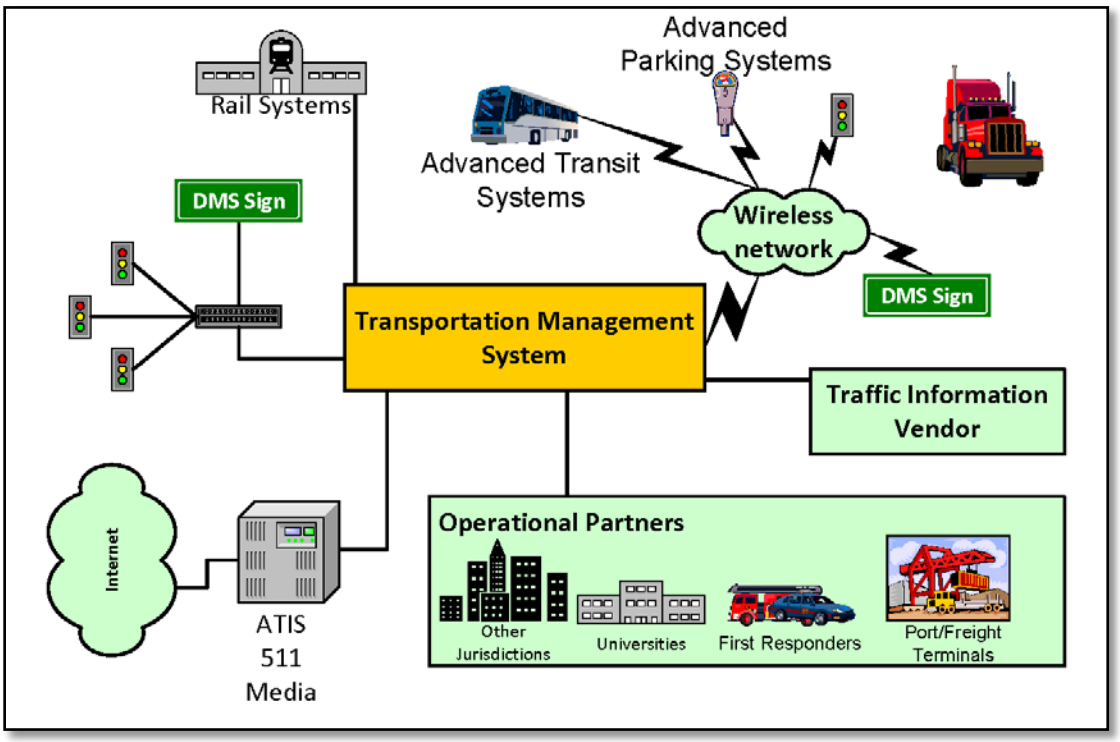

Figure 5: Relationship between Traffic Signal Control Systems, Traffic Management Systems, and the Highway/Roadway Network[13]

Key ITS elements in the Highway Mode include:

- Use of old legacy control devices,
- Upgrade and migration entail layering of modern IT and meshing of telecommunications systems, with increasing reliance on wireless protocols,
- Integration between different transportation operators' systems (including those used in passenger rail) along with shared use of telecommunications networks, and
- Location of much of the distributed ITS network in public domain areas.

[13] Source: "National ITS Architecture Subsystems and Communications," courtesy of the Federal Transit Administration.

Modern ITS also includes many different field devices that are on the front lines of transportation management, delivering sensor information from throughout a region's transportation network over multiple communications networks to various transportation management centers and receiving command and control instructions in response. Types of traffic control system devices include ramp/gate/signal controllers, fixed and portable dynamic message signs, enforcement systems, smart parking management systems, and embedded devices. In some parts of the county, the information network includes distribution to individual consumers via advanced traveler information systems (ATISs); these systems deliver real-time, current traffic, weather, and other travel-related information to cars, drivers, and other travelers. Effective communication with the public is one of the most important elements in effective operation of a modern transportation facility.

Figure 6: Traffic Signal Control Box[14]

The use of advanced computing, sensing, and communication technologies will continue to support transportation systems to meet the increasing operational challenges on the national ground transportation network. Each technological advance brings additional capabilities to meet the objective of transportation agencies, but can also increase the attack surface of these systems. The world today is very different than it was when ITS began over 20 years ago; now, it is very important that agency owners include system security and protection in their design and maintenance responsibilities to ensure continuity of service and protection of critical support functions.

[14] Source: Photograph provided courtesy of FHWA/California DOT.

6.4 Maritime Mode

The Maritime Mode includes a wide range of watercraft and vessels and consists of approximately 95,000 miles of coastline, 361 ports, 10,000 miles of navigable waterways, 3.4 million square miles of the Exclusive Economic Zone, and intermodal landside connections, which allow the various modes of transportation to move people and goods to, from, and on the water.[15]

The Maritime Mode can be divided into two sectors: vessels and ports. Vessels include dry bulk carriers, petroleum and chemical tankers, containerships, general cargo ships, roll-on roll-off ships, ferries and passenger ships, river vessels, tugboats, towboats, barges, commercial fishing vessels, workboats, special purpose vessels, and recreational vessels.

Maritime Vessels

Dry bulk carriers are vessels designed to transport unpackaged bulk cargo, such as grains, coal, ore, and cement, in their cargo holds.

Tankers are ships designed to transport liquids, such as oil, petroleum, chemical, etc., in bulk.

Containerships are vessels that carry their loads in reusable intermodal containers, also known as ISO containers. ISO containers are steel containers measured in twenty-foot equivalent units (TEUs), which is a unit of capacity equal to one standard 20 foot (length) times 8 foot (width) container. These containers can be moved from one mode of transport to another without unloading and reloading the container's contents.

General cargo ships are vessels that carry cargo, produce, goods, and materials from one port to another. Typically, cargo is loaded to and unloaded from these ships via the use of cranes.

Roll-on roll-off ships are vessels designed to carry wheeled cargo, such as automobiles, trucks, trailers, etc., that are driven on and off the ship on their own wheels via built-in ship ramps.

Ferries/passenger ships are vessels whose primary purpose is to carry passengers (and sometimes vehicles and cargo) across a body of water.

River vessels are boats designed for inland navigation on lakes, rivers, and artificial waterways. They may transport passengers and/or cargo, or may serve as special purpose vessels.

Tugboats and towboats are vessels that maneuver unpowered vessels by pushing or towing them or that assist with the maneuvering of deep draft vessels during their transit in or out of port.

Barges are flat-bottomed vessels built mainly for coastal, river, and canal transport of heavy goods, bulk materials, and liquid bulk cargos.

Fishing vessels include commercial and recreational boats and ships used to catch fish in a sea, lake, or river.

Workboats and special purpose vessels are ships designed to perform specialized tasks, such as drilling for oil, laying cables, serving as fireboats, etc., while on the water.

Recreational vessels are those manufactured or operated primarily for pleasure, or leased, rented, or chartered to another for his/her pleasure.

Sources: Wikipedia and 46 USCS Section 2101; URL at: www.uslegal.com

[15] DHS, *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010, Table 1-1.

U.S. ports are categorized as international seaports, coastal ports, Great Lakes, and marine highway ports. U.S. port authorities act as operating ports, landlord ports, or a combination of the two. Operating port authorities manage all of the cargo operations at their terminals; landlord port authorities lease terminals to private sector stevedore companies that manage all of the cargo operations, including the hiring of longshore labor personnel to load and unload ships. Port security involves the use of various types of communications systems (generally radio or cell phone), sensor systems (such as radar, underwater detection, and remote cameras), and command and control information management systems.

Several types of terminals may be present within each port or harbor. Types of terminals include general purpose cargo terminals, container terminals, dry bulk cargo terminals, petroleum terminals, chemical and liquid cargo terminals, fishing boat terminals, workboat terminals or piers, and passenger vessel terminals, which include ferries, cruise ships, and party boats. The terminal composition of an individual port will depend on the types of cargo or passenger ships that call on that port. Detailed information regarding a port's terminals is usually available on the port's website. Security for individual terminals is conducted by the terminal operator, and includes the use of security cameras, access control systems, and radio communications systems.

The terminal operational layout is designed, or has special equipment, to load and offload the particular type of cargo it services and to provide access for the particular type of vessel that carries the cargo. Many smaller ports and terminals for local fishing and entertainment, both commercial and public, also exist.

Control systems for vessels include communication systems; navigation systems; main engine, generators, ballast, and other tanks; fuel and lube oil systems; cargo hold fans; water-tight door controls; and vessel life support systems. The container terminal inventory includes automation at truck entrances and exits; communications; information technology systems; terminal operating systems; and control systems on ship-to-shore cranes, rubber tire gantry cranes, yard cranes, and yard equipment.

Figure 7: Vessel System and Engine Control Panels (on ship)[16]

[16] Source: Volpe project photograph.

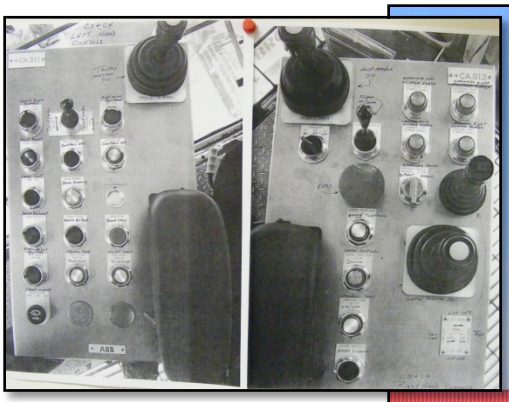

Figure 8: Ship-to-Shore Crane Remote Controls[17]

Figure 9: Ship-to-Shore Cranes at a Terminal[18]

The following description of vessel traffic services (VTSs) is excerpted from the USCG's Navigation Center website.[19]

USCG operates 12 Vessel Traffic Centers (VTCs) positioned strategically throughout the U.S. These VTCs provide VTSs with active monitoring and navigational advice for vessels in particularly confined and busy waterways. There are two main types of VTSs, surveilled and non-surveilled. Surveilled systems consist of one or more land-based sensors (i.e. radar, automatic identification systems (AISs), and closed circuit television sites), which output their signals to a central location where operators monitor and manage vessel traffic movement. Non-surveilled systems consist of one or more reporting points at which ships are required to report their identity, course, speed, and other data to the monitoring authority. They encompass a wide range of techniques and capabilities aimed at preventing vessel collisions, rammings, and groundings in and around the harbor. They are also designed to expedite ship movements, increase transportation system efficiency, and improve all-weather operating capability.

VHF-FM communications network forms the basis of most major services. Transiting vessels make position reports to a vessel traffic center by radiotelephone and are in turn provided with accurate, complete, and timely navigational safety information. The addition of a network of radars, AIS, and close circuit television cameras for surveillance and computer-assisted tracking, similar to that used in air traffic control, allows the VTS to play a more significant role in marine traffic management, thereby decreasing vessel congestion, critical encounter situations, and the probability of a marine casualty resulting in environmental damage.

[17] Source: Volpe project photograph.
[18] Source: Volpe project photograph.
[19] URL Source: http://www.navcen.uscg.gov/?pageName=vtsMain.

6.5 Pipeline Mode

The Pipeline Mode includes pipeline networks, operated by more than 3,000 operators, which traverse millions of miles throughout the U.S. This mode includes city gate stations, distribution networks, and terminals that transport and distribute nearly all of the Nation's natural gas and about 65 percent of the nation's hazardous liquids, in addition to other chemicals.[20]

The pipeline industry is comprised of hundreds of companies which own and operate more than two million miles of pipelines. While the predominance of America's pipelines carry natural gas, some carry a wide variety of other gases or liquids, primarily energy products in various states of refinement. Many of these are highly volatile and accidents can have catastrophic consequences. Others, while less volatile, are nonetheless essential to the stability of the nation's economy.

There are 2.3 million miles of gas and liquid petroleum pipelines in the United States. About 87 percent of these pipelines deliver natural gas from many sources through a vast network to more than 70 million individual homes. In spite of how densely covered the map in Figure 10 appears, it shows only the gathering and transmission natural gas pipelines in the U.S. Distribution pipelines represent the vast majority of the nation's pipelines, and they are not shown on the map.

Pipeline Terminology

City Gate: A site at which a gas distribution company receives gas from a pipeline company or transmission system.

Distribution: The act or process of distributing natural gas from the city gate station to the ultimate consumers.

Distribution System: The mains, services, and associated equipment that carry or control the gas supply from the point of local supply to and including the sales meters of the consumers.

Operator: An entity engaging in the transportation of natural gas or hazardous liquids. Operators are responsible for operating and maintaining pipeline systems.

Pipeline: Continuous pipe conduit, complete with other equipment (such as valves, tanks, and pressure control devices) for transporting fluids or gases from one point to another. Pipelines generally fall into three categories:

- Gathering pipelines transport commodities from their sources to refineries.
- Transportation pipelines move commodities over long distances from refineries or large storage facilities to distributors.
- Distribution pipelines deliver commodities (mostly natural gas) to customers' homes or businesses.

Transmission Line: Pipeline installed for transporting large quantities of product from source(s) of supply to one or more distribution centers, distribution systems, or large volume customers (e.g., power generation plants). Typically, transmission lines are longer, larger in diameter, operate at much higher pressures, and have greater distances between connections than distribution lines.

URL Source:
www.phmsa.gov/staticfiles/PHMSA/Pipeline/Intro_to_Pipeline/iz_00.htm

[20] DHS, *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010, Table 1-1.

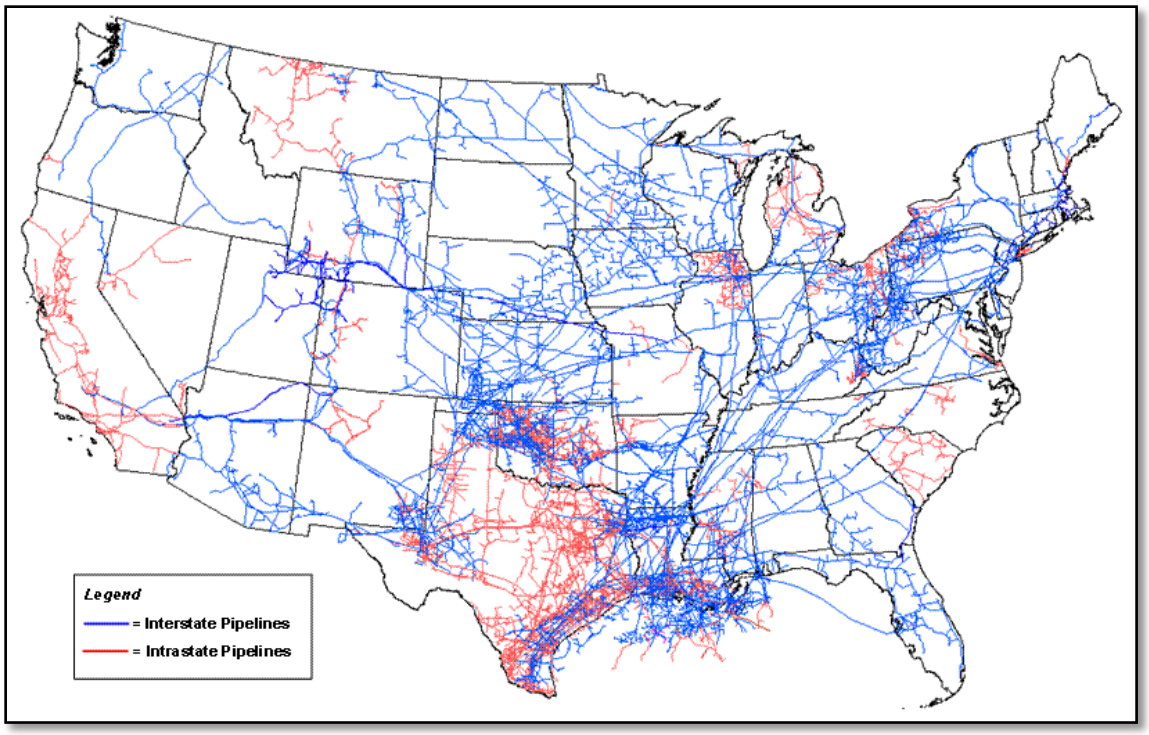

Figure 10: U.S. Gathering and Transmission Natural Gas Pipelines[21]

Probably more than any transportation mode, the Pipeline Mode is reliant on control systems for its operation. The industry is highly automated, and the reliable operation of its control systems is critical in preventing potentially catastrophic situations. Control systems in the pipeline industry include hundreds of SCADA systems, thousands of remote terminal units (RTUs), and approximately one million controllable devices. The industry is migrating toward a more connected control infrastructure and is increasingly vulnerable to attacks on its control systems.

[21] Source: Energy Information Administration, Office of Oil & Gas, Natural Gas Division, Gas Transportation Information System.

Figure 11 illustrates the general features of a natural gas distribution pipeline facility, and Figure 12 shows the associated control and communications system.

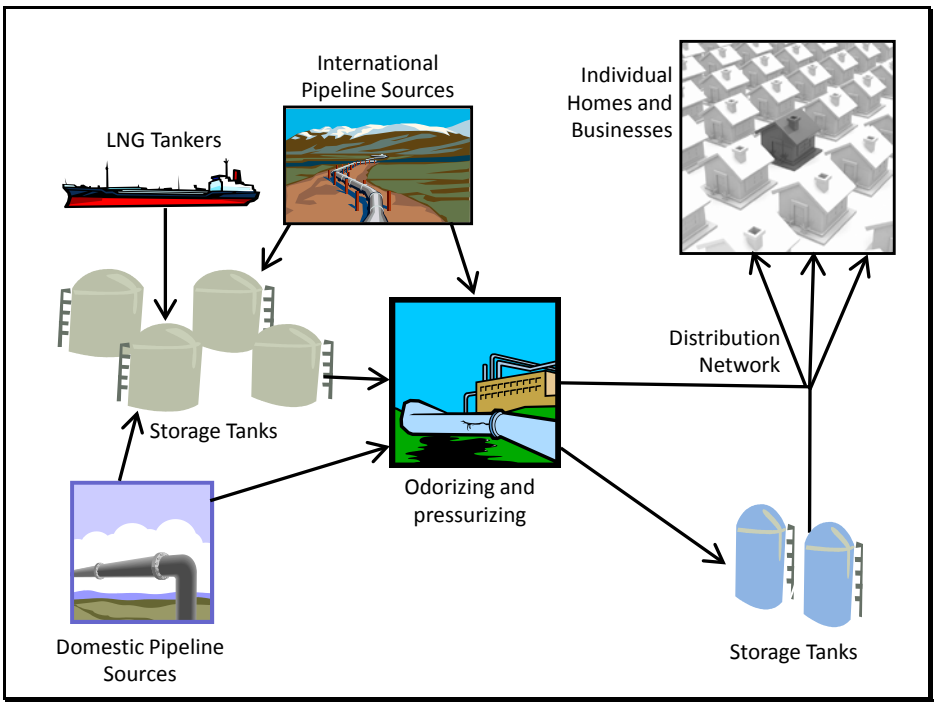

Figure 11: Notional Example of a Natural Gas Distribution Pipeline Facility

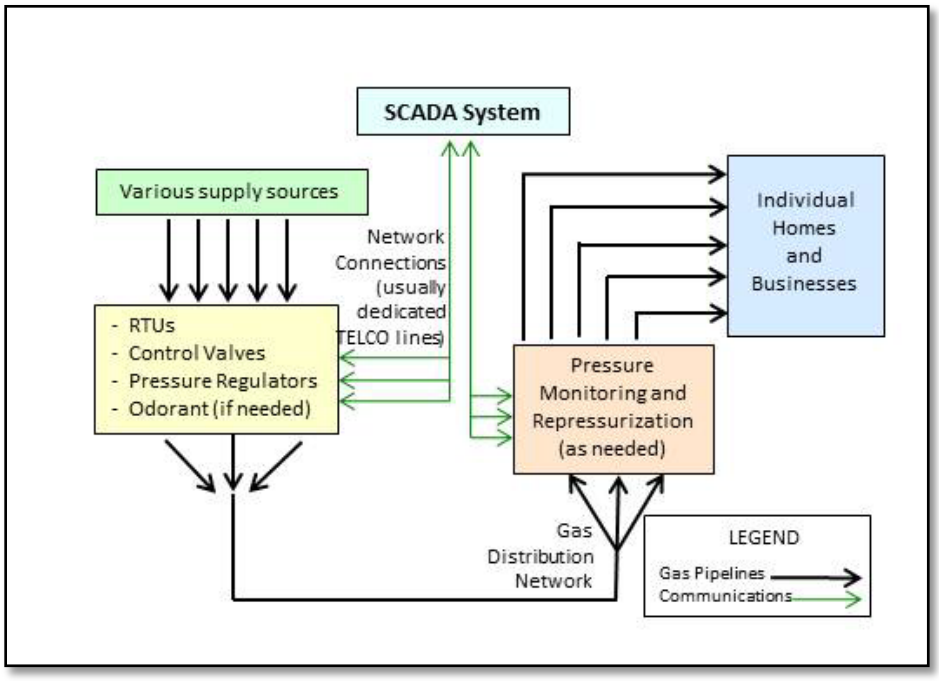

Figure 12: Notional Layout of a Company's Control and Communication System

While the sources for commodities transported by pipelines are defined and small in number, the customers are usually vast in number. In general, SCADA systems are used to ensure that the acceptable commodity pressure range is maintained; to provide alerts for suboptimal conditions (e.g., leaks, improper level of odorant additives; commodity temperature outside of acceptable range); and to ensure that the provider company is drawing commodity from the preferred source (e.g., least expensive), based on the company's business models and projections. RTUs in the pipeline industry are generally located at the commodity injection points, where they monitor flow, pressure, temperature, odorant, as well as perform other company-specific commodity distribution functions. Controllable devices, including pressure regulators and control valves placed at various strategic locations throughout the company's distribution network, are myriad and serve various purposes. Typically, these devices never need to be adjusted: once in the field, they typically remain at a fixed setting for their entire operational lives. The only exception is when a leak or explosion occurs, at which point the control valve is shut off to prevent the commodity from flowing through the affected part of the pipeline infrastructure.

6.6 Surface Transportation Mode

The Surface Transportation Mode consists of freight rail and passenger rail (also referred to as public or mass transit).

6.6.1 Freight Rail

Freight rail is comprised of seven major carriers (Class I), hundreds of smaller railroads (Class II and III), over 140,000 miles of active railroad, more than 1.3 million freight cars, and approximately 20,000 locomotives. Daily, more than 12,000 freight trains are in operation. The Department of Defense (DOD) has designated 30,000 miles of track and structure as critical to mobilization and resupply of U.S. forces.[22]

Railroads are classified according to revenues generated. U.S. Class I Railroads are line haul freight railroads with 2010 operating revenue of $398.7 million or more. The seven Class I Railroads operating in the U.S. are BNSF Railway Company, CSX Transportation, Grand Trunk Corporation, Kansas City Southern Railway Company, Norfolk Southern Combined Railroad Subsidiaries, SOO Line Railroad Company, and Union Pacific Railroad.

URL Source: American Association of Railroads, http://www.aar.org/~/media/aar/Industry%20Info/AAR-Stats-2012-05-10.ashx.

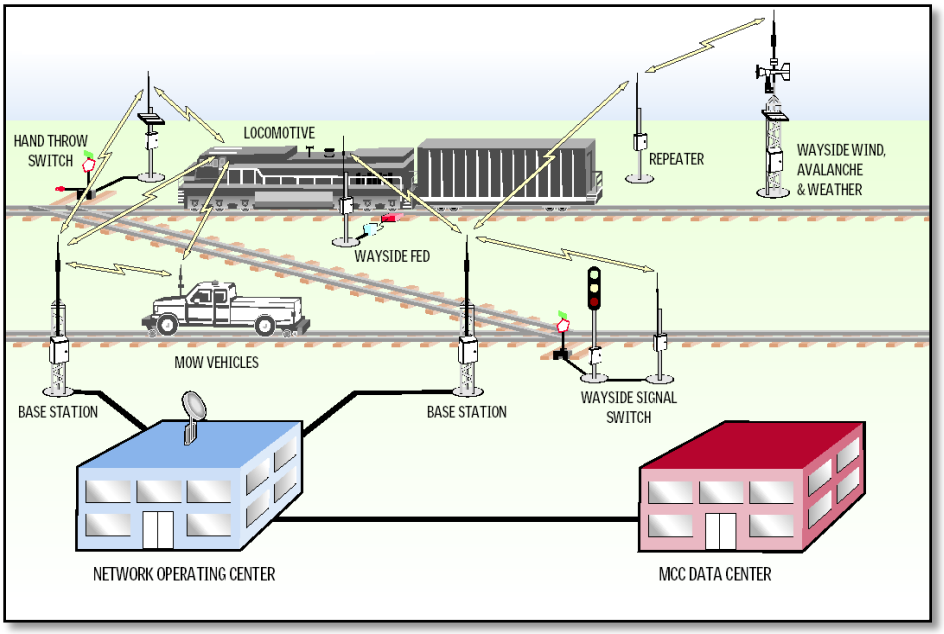

Figure 13: Notional Positive Train Control Systems

[22] DHS, *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010.

U.S. railroads are entering a period of massive change. Economic pressures, aging equipment, operational efficiencies, and legislation such as Public Law 110-432, which mandates the widespread installation of positive train control (PTC) systems by December 2015, are causing the railroad industry to increasingly look to technological solutions. PTCs, yard control and automation systems, electronically controlled pneumatic (ECP) brakes, interlocking controls, locomotive remote controls, and on-board network systems are some of the control system technologies that are being incorporated into today's railroads. Interoperability, uniform standards, and compatibility with existing equipment are some of the physical challenges that the rail industry continues to face. Along with the new technologies that the railroads are employing, cyber security of railroads' vital control systems should be considered an integral part of security.

Surface Transportation Terminology

PTCs are systems where the train receives information about its location and where it is allowed to safely travel. Equipment on board the train enforces this information, thereby preventing unsafe movement. PTC systems may work in either signaled or dark (i.e., non-signaled) territory and may use GPS navigation to track train movements.

Yard control and automation systems control the storage, sorting, loading, and unloading of railroad cars and locomotives at a rail yard. These systems include track controls, switch locomotives (used to move railroad cars around the rail yard), towers with control equipment, and other devices and equipment.

ECP brakes are a type of modern railway braking system that improves braking performance over traditional pneumatic (compressed air) brakes. While traditional systems apply the brakes sequentially from car to car along a train, ECP brake systems use microprocessor controlled valves to activate brakes simultaneously to all train cars. This uniform and instantaneously brake application allows for better train control, shortens the train's stopping distance, and decreases the risk of derailments or coupling breakage.

Interlocking controls are electronic signaling system arrangements designed and interconnected to prevent conflicting movements through an arrangement of tracks, such as those at junctions and crossings. Interlockings are designed to move in proper sequence, thus making it impossible to give clear signals to trains unless the intended route is proven to be safe.

Locomotive remote controls provide motive power for trains by use of a remote control radio transmitter and receiver system that is used to operate the locomotive by a person not physically located in the locomotive's cab. These systems are designed to be fail-safe; if communication is lost, the locomotive is automatically stopped.

On-board network systems include controls for bus and communications, safety, diagnostics, energy and service, desk and drive, information and entertainment, and train platform doors.

Sources: Wikipedia and URL: www.railway-technology.com/contractors/computer/far-systems

6.6.2 Passenger Rail / Public Transit

Passenger rail/public transit includes multiple-occupancy vehicles designed to transport customers on regional and local routes. Passenger rail/public transit vehicles include transit buses, trolleybuses, monorails, light rail, subways, commuter rails, long-distance rails, automated guide-way transit, inclined planes, and cable cars.[23] Each of these vehicle types has associated passenger and support facilities, which in turn will have associated control systems.

Passenger Rail / Public Transit Vehicles and Systems

Transit buses, also known as commuter buses, city buses, or public buses, are buses used for short-distance public transport purposes.

Trolleybuses are electric buses that draw their electricity from overhead wires (generally suspended from roadside posts) using spring-loaded trolley poles. Two wires and poles are required to complete the electrical circuit.

Light rail is a term used to refer to rail systems with rapid transit-style features that usually use electric rail cars operating mostly in private rights-of-way separated from other traffic. Light rail generally has lower capacity and slower speed than heavy rail and metro systems, but higher capacity and faster speed than street-running tram systems.

Monorails are rail-based transportation systems based on a single rail, which acts as its sole support and guideway.

Subways are rapid transit electric passenger railways located in urban areas with high capacity and frequency and grade separation from other traffic. Subways are typically located either in underground tunnels or on elevated rails above street level.

Commuter rails are passenger rail transport services that primarily operate between a city center and the middle to outer suburbs and commuter towns or other locations that draw large numbers of people who -travel on a daily basis.

Long-distance rails travel between many cities and/or regions of a country, and sometimes cross several countries. They often have a dining or restaurant car to allow passengers to have a meal during the course of their journey.

Automated guide-way transit systems are fully automated, driverless, grade-separated transit systems in which vehicles automatically travel along a guideway.

Inclined planes are straight ramps cut into a hillside and used for moving loads up and down the hill. Inclined planes are often provided with cars riding on rails and pulled up and lowered down using a cable drive system powered by a steam engine.

Cable cars are a variety of transportation systems relying on cables to pull vehicles along or lower then at a steady state, or a vehicle on these systems.

Source: Wikipedia

[23] DHS, *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010, Table 1-1.

Figure 14: Underground Subway[24]

Because passenger rail/public transit includes a wide variety of vehicles and equipment travelling over dedicated pathways, central control and monitoring of all aspects of the transit network is critical to maintaining operational control in this mode. Control systems in passenger rail/public transit can be described both by their common designations and by the functions they perform. Some control systems provide a specific function (e.g., train control), whereas others integrate different functions (e.g., emergency alarms, fire detection, gas monitoring) into one or more enhanced systems. Passenger rail/public transit control systems can be grouped into the following six main system types:[25]

- **Control systems** include train control systems and SCADA systems. Train control systems are used to operate underground and surface public transit vehicles. These systems may operate in either a semi-autonomous mode (used for underground travel) or a speed limited manual mode (when traveling on streets and other aboveground surfaces). They include equipment in the trains and buses as well as along the route (e.g., traffic lights, gates, etc.). SCADA systems control the supply of power to transit stations (used to operate building management aspects such as fire life safety, HVAC, intrusion detection, etc., equipment) and to move the actual passenger trains. Such systems often link each transit station to others along the transit route, and provide remote control and monitoring of associated field equipment.

[24] Source: Volpe project photograph.

[25] APTA, *Draft Technical Recommended Practice for Securing Control and Communications Systems in Transit Environments: Part 1 - Elements, Organization and Risk Assessment/Management*, Version 1.0.9, August 31, 2009.

- **Communication systems** include radio, closed circuit television (CCTV), intercom, public information displays, and public address systems used to provide transit passenger with transportation information such as estimated arrival time, delays, emergency directives, etc.

- **Security control systems** include CCTV, intrusion detection, video surveillance, alarm, and other monitoring systems designed to provide real-time views of the various system assets such as platforms, station lobbies, etc. These systems are usually connected to an operations center, where recorded information is monitored and stored.

Figure 15: Passenger Access Control Gates at a Subway[26]

- **Data transmission systems** include fiber optic networks, copper networks, leased lines, and wireless network systems that provide the data communications infrastructure between a transit agency's control center and other transit buildings and properties and for local area networks (LANs) and wide area networks (WANs).

- **Fare collection systems** are used to collect transit payments from fare collection devices at each station. Fare collection systems can often support point-of-sale devices situated in locations not directly controlled by the transit authority and wireless fare card verification devices located throughout the transit system. These systems are often integrated with entry/exit gates, station access points/garages, etc., and are frequently linked with financial systems and the governing transit agency's back office functions.

[26] Source: Volpe project photograph.

- **Vehicle monitoring systems** refer to control systems, similar to those for train control, used for automatic vehicle monitoring of buses, streetcars, and other surface systems, including non-revenue equipment.

Many public transit agencies provide more than one transportation mode and when they do, each mode is operated practically autonomously. In addition, passenger rail/public transit has a variety of other cybersecurity challenges, including:

Different Control Systems. Control systems may be completely different. For example, bus operations will typically have GPS-based automated vehicle location systems which simply "track" bus movement whereas rail will have various means of controlling track switches and sometimes include automatic functions to control train power, routing, and speed.

Separate Network and Communications Teams. The business/management division and the modes often have their own network and communications engineers. For example, the business/management division may have a dedicated IT staff to manage the IT network and workstations while each mode may have its own control system engineers to build its own networks to support its control systems. These separate teams can result in different security practices and standards being implemented for networks and communications.

Shared Communications Backbone. To tie together the different modes, a shared network and communications backbone is often used. This backbone is often deployed and managed by rail control systems engineers to support the train control systems, but the entire agency may use the backbones as the core of its WAN. Such a scenario results in networks and control systems with different security practices and standards operating on the same WAN.

Legacy Control Systems on Modern Networks and Being Replaced by IP-Based Control Systems. Most transit agencies have already used modems to convert legacy analog control signals to digital signals to take advantage of WANs and to extend the reach of their controllers. Many agencies are also making incremental upgrades to their control systems by replacing legacy analog controllers with digital and IP-based controllers. Public transportation is replacing its legacy control systems, often isolated from other industry systems, with next generation control systems based on traditional IT technologies that rely on networks, wireless communications, GPS, and microprocessor-based devices. While there are many benefits to these practices, an unintended consequence is that systems previously immune to cyber vulnerabilities are now vulnerable to cybersecurity attacks.

IP-Based Security Systems Driving the Design of Agency WANs. Physical safety and security are vital to transit agencies and most have or are deploying agency-wide security measures including IP-based access control systems and IP-based video surveillance. These security systems are driving the design of WANs and significantly increasing the number of IP-based edge devices on transit agency networks.

7.0 Goals, Objectives, Metrics and Milestones

This section presents four strategic goals designed to assist transportation professionals in focusing activities and resources for improving the cybersecurity of ICS. These goals provide a logical framework for organizing the collective efforts of the transportation industry, government, and other key stakeholders for achieving ICS cybersecurity. The goals are broad-based, applicable to all transportation modes and organizations, developed around a 10-year outlook, and designed to be achieved concurrently. When viewed together, the four goals are intended to capture the full spectrum of activities needed for transportation control systems cybersecurity.

Near-term (0-2 years), mid-term (2-5 years), and long-term (5-10 years) objectives, with corresponding milestones and metrics (i.e., Near-Term Objective "a" matches with Near-Term Milestone and Metric "a")[27], are presented for each goal. This information gives organizations specific activities to conduct to better secure transportation ICSs, and provides corresponding milestones and metrics for individual organizations to use for determining whether they have achieved the objective. Because this Transportation Roadmap is developed to be applicable to the whole Transportation Sector as well as to individual modes and organizations, the milestones and metrics also provide broad quantification information each mode, and the Transportation Sector, can use to determine the mode's/Sector's progress as a whole towards achieving the corresponding objective.

The four Transportation Roadmap goals, and their corresponding end states, are:

Goal 1: Build a Culture of Cybersecurity
End State: Cybersecurity and ICS are viewed as inseparable and integrated throughout the Transportation Sector.

Goal 2: Assess and Monitor Risk
End State: The Transportation Sector has a robust portfolio of ICS-recommended security analysis tools to effectively assess and monitor ICS cybersecurity risk.

Goal 3: Develop and Implement Risk Reduction and Mitigation Measures
End State: Security solutions for legacy systems, new architectural designs, and secured communication systems in the Transportation Sector are readily available and deployed across the Sector.

Goal 4: Manage Incidents
End State: The Transportation Sector is quickly alerted of cybersecurity ICS incidents, and sophisticated, effective, and efficient mitigation strategies are implemented and in operation.

[27] While Objectives within each timeframe (Near-, Mid-, and Long-Term) match to the corresponding Milestone and Metric in the same timeframe, Objectives (and thus Milestones and Metrics) between timeframes are not designed to match (e.g., Mid-Term Objective "a" is not intended to match with Near- and Long-Term Objective "a").

The information presented in this section should be viewed as a starting point for enhancing transportation ICS cybersecurity; as each organization, transportation mode, and the Transportation Sector itself improves its cybersecurity posture, new objectives, milestones, and metrics should be developed based on the current cybersecurity threats and risks. Similarly, this information can be used by individual transportation modes and organizations to develop modal and organization-specific roadmaps for securing ICSs.

Goal 1: Build a Culture of Cybersecurity

	Objectives	Milestones and Metrics
Near-Term (0-2 years)	a. Develop and implement an ICS cybersecurity governance model. b. Identify roles and responsibilities, structure, and authorities for ICS cybersecurity planning and risk management. c. Educate transportation executives on the importance of ICS cybersecurity. d. Establish ICS cybersecurity policies and procedures, resources, and budget/funding. e. Develop a cybersecurity awareness training program, and begin delivering it to new hires and existing employees.	a. The organization has a documented ICS cybersecurity business case. b. Personnel have been formally assigned ICS cybersecurity planning and risk management responsibilities and budgets. c. Many transportation executives recognize ICS cybersecurity as mission critical. d. The organization has identified the ICS policies and procedures it will follow, and has established the necessary ICS resources and budget/funding. e. A formal cybersecurity awareness program is developed, and the organization has begun to deliver the training to its employees.
Mid-Term (2-5 years)	a. Refine the cybersecurity awareness training program by increasing the depth of information provided and the extent of employees trained. b. Institutionalize cybersecurity language/methodologies in ICS contracts, user agreements, statements of work, asset management procedures, etc. c. Develop a robust ICS self-assessment program/business case. d. Develop security assessment capabilities for new and legacy ICSs. e. Establish a mechanism that allows for frequent and ongoing collaboration between operations and security cyber staff and ICS operators and engineers.	a. The organization has further developed its cybersecurity awareness training program, and has provided the training to many of its employees. b. Most ICS-related procurements, documents, procedures, and policies include provisions for cybersecurity. c. Asset owners and operators perform self-assessments of most of their ICSs according to the frequency identified in their associated program/business case. d. The organization identifies its current security assessment capabilities for new and legacy ICSs, including the types of assessment tools utilized. e. The organization has established a formal means for periodic collaboration between operations and security cyber staff and ICS operators and engineers.
Long-Term (5-10 years)	a. Establish automated processes to secure ICSs. b. Ensure that cybersecurity awareness training is periodically updated and provided to personnel at all organizational levels. c. Incorporate cybersecurity language, reviews, and considerations into all levels of ICS-related business practices and budgetary considerations. d. Establish ISACs (or equivalent) for each transportation mode and for the Transportation Sector.	a. Most ICSs are continuously monitored via established automated processes. b. The organization has an established process for updating its cybersecurity awareness training, with most staff receiving annual cybersecurity awareness refresher training. c. Cybersecurity is integrated into most ICS business practices. d. Modal ISACs, together with a Transportation Sector ISAC (or equivalent), serve as the conduit of cross-modal lessons learned and best practices in ICS cybersecurity, and provide a forum for partnership, outreach, and information sharing within each mode and throughout the Transportation Sector.
End State:	**Cybersecurity and ICS are viewed as inseparable and integrated throughout the Transportation Sector.**	

Goal 2: Assess and Monitor Risk

	Objectives	Milestones and Metrics
Near-Term (0-2 years)	a. Identify risk management framework and standards. b. Identify common metrics for benchmarking ICS risk (threats-vulnerabilities-consequences). c. Integrate cybersecurity into business functions and operation plans. d. Develop and disseminate ICS risk assessment and reporting standards and guidelines that enable cybersecurity tools and metrics to be effectively deployed. e. Identify cybersecurity risk management roles and responsibilities, including establishing authorities responsible for accepting and mitigating cybersecurity risk. f. Adopt and deploy cybersecurity posture assessment tools (Cybersecurity Evaluation Tool (CSET) or equivalent) for ICS cybersecurity vulnerability assessments.	a. Each organization identifies the risk management framework and standards it will follow. b. Each organization prioritizes its identified ICS cybersecurity risks based on defined common metrics. c. All business functions and operation plans contain a cybersecurity component. d. ICS risk assessment and reporting guidelines are published and disseminated throughout each organization. e. All asset owners and operators have identified personnel responsible for ICS cybersecurity risk management. f. Many asset owners and operators have deployed cybersecurity posture assessment tools (CSET or equivalent).
Mid-Term (2-5 years)	a. Develop and implement a risk management model and strategy. b. Develop and implement a risk assessment program, with considerations for both top-down and bottom-up approaches. c. Examine and test the use of automated tool options for ICSs. d. Examine and assess real-time security assessment capabilities for new and, where appropriate, legacy systems. e. Develop and implement a cyber risk management training program for personnel with cybersecurity responsibilities.	a. Each organization identifies the risk management model and strategy it will use. b. Most asset owners and operators have implemented a cybersecurity ICS risk assessment program, with considerations for both top-down and bottom-up approaches. c. Most owners and operator have examined and tested the use of automated tool options for ICSs. d. Real-time security assessment capabilities have been reviewed for most ICSs (new and legacy). e. Many employees with ICS responsibilities receive specialized cybersecurity training that includes instruction on risk assessment tools aligned with the organization's risk management model, strategy, framework, and standards.
Long-Term (5-10 years)	a. Establish a formal risk management program. b. Establish and implement a continuous and automated risk monitoring program, including tools, for ICSs. c. Incorporate risk management considerations into all levels of ICS cybersecurity (contracts, user agreements, purchases, etc.). d. Establish, and regularly use, communication mechanisms for measuring risk management performance and benchmarking among the transportation modes and with other sectors. e. Develop and implement a cybersecurity ICS training program review process.	a. Each organization has established a formal risk management program, including related processes, for risk measurement and reporting. b. Most asset owners and operators are using continuous and automated ICS risk monitoring programs and tools. c. Cybersecurity is integrated into most ICS business practices. d. Each transportation mode has an active program for ICS security profile assessment, and regularly shares this information, for benchmarking purposes, with other modes and sectors. e. Each organization has established and implemented a review process for monitoring its cybersecurity ICS training program.
End State:	**The Transportation Sector has a robust portfolio of ICS-recommended security analysis tools to effectively assess and monitor ICS cybersecurity risk.**	

Goal 3: Develop and Implement Risk Reduction and Mitigation Measures

	Objectives	Milestones and Metrics
Near-Term (0-2 years)	a. Develop and disseminate ICS protection guidelines that assist in ensuring existing access controls are properly implemented and enabled. b. Develop a template protocol for responding to cyber incidents. c. Establish mechanisms for sharing information between asset owners, operators, and vendors to develop improved protection tools. d. Identify, implement, and maintain, where appropriate, existing built-in cybersecurity features in ICS equipment. e. Encourage/prioritize that ICS vendors begin implementing or improving their equipment's cybersecurity features. f. Develop, implement, and maintain cybersecurity measures—including items such as firewalls, intrusion detection, passcodes, anti-virus protection, and patching technologies—having minimum host impact and without compromising safety. g. Train employees on the ICS protection guidelines. h. Analyze the organization's current cybersecurity posture with respect to its compatibility with existing and new technologies.	a. ICS protection guidelines have been developed and disseminated throughout the organization. b. Many asset owners and operators have developed and implemented cyber incident response protocols. c. Each organization has established a process for sharing cybersecurity protection information among asset owners, operators, and vendors. d. Most asset owners and operators have identified cybersecurity features built into their control systems, and many have implemented these features, where appropriate. e. Each organization has established a preference for vendors offering equipment with enhanced cybersecurity features. f. Some asset owners and operators have begun implementing enhanced cybersecurity measures. g. Most organizations have trained their employees on their ICS protection guidelines. h. Each organization has conducted an analysis of its current cybersecurity posture, while considering compatibility with existing and new technologies.
Mid-Term (2-5 years)	a. Reduce time required for ICS patch installation. b. Develop provisions for accommodating restarts in control systems design. c. Implement and maintain effective ICS cybersecurity protection tools. d. Secure most of the interfaces between ICS and internal and external systems. e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs. f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.	a. Each organization has reduced its average patch installation time. b. Each organization has established provisions for accommodating control system restarts at the design level. c. Each organization has implemented and is maintaining effective cybersecurity protection tools for ICSs. d. Asset owners and operators have established secure interfaces between most ICSs and internal and external systems. e. Many operators have completed a cybersecurity training program that includes information on the protection tools and features used to secure ICSs. f. Many asset owners and operators have performed nondisruptive ICS intrusion tests.
Long-Term (5-10 years)	a. Plan for and integrate cyber-resilient ICS architectures and infrastructure that have built-in, self-defending security, and use and maintain systems and components that are secured-by-design. b. Identify best practices for connecting ICSs and business networks. c. Secure all of the interfaces between ICSs and internal and external systems. d. Ensure that most operators receive specialized cybersecurity training commensurate with their respective duties and responsibilities. e. Encourage/prioritize that real-time monitoring tools for cybersecurity intrusions are commercially available.	a. Secure ICS architectures with built-in, end-to-end security are in all of the organization's critical ICSs. b. Each transportation mode has developed best practices for securely connecting ICSs and business networks, where appropriate. c. Asset owners and operators have established secure interfaces between all ICSs and internal and external systems. d. Most operators have received ICS cybersecurity training commensurate with their respective duties and responsibilities. e. Each mode has established formal working relationships with industry, and has promoted the development of COTS tools that provide real-time monitoring for ICS cybersecurity intrusions.
End State:	**Security solutions for legacy systems, new architecture designs, and secured communications systems in the Transportation Sector are readily available and deployed across the Sector.**	

Goal 4: Manage Incidents

	Objectives	Milestones and Metrics
Near-Term (0-2 years)	a. Develop and deploy sensors and systems to detect and report abnormal activity. b. Identify recommended practices and approved guidelines for incident reporting and information sharing of ICS cybersecurity-related events. c. Begin developing and implementing associated continuous improvement mechanisms for incident reporting and Information sharing, and establish a process for disseminating the updated information to stakeholders. d. Develop and incorporate cyber incident response and recovery planning into established business continuity plans. e. Develop procedures for responding to ICS incidents, and provide employees with training on response procedures for ICS incidents commensurate with their roles and responsibilities. f. Work with vendors on specifications for new ICS detection and response tools and equipment.	a. Some asset owners and operators have deployed sensors and systems for detecting and reporting abnormal ICS activity. b. Each organization has identified the practices and guidelines for incident reporting and information sharing it will follow for managing ICS cybersecurity-related events. c. Each organization has begun developing and implementing continuous improvement mechanisms for incident reporting and information sharing, and has established a process for disseminating the updated information to its stakeholders, as appropriate. d. Some asset owners and operators have incorporated a cyber incident response and recovery planning component into their established business continuity plans. e. Most asset owners and operators have developed ICS incident response procedures, and some have provided employees with ICS incident response training commensurate with their roles and responsibilities. f. Many organizations have established formal working relationships with industry for developing specifications for new/improved ICS detection and response tools and equipment.
Mid-Term (2-5 years)	a. Research and implement new, improved, and more effective detection, response, and recovery tools and equipment. b. Establish procedures for the periodic upgrade of business continuity plans and training programs to reflect changes in new tools, equipment, and recommended ICS practices. c. Develop and implement employee training programs that provide specialized instruction on the implementation of new ICS tools and procedures, based on employee roles and responsibilities. d. Develop public communication strategies regarding the potential consequences of transportation network disruption from a cyber incident.	a. Each organization has established a process for identifying, vetting, and implementing, where appropriate, new, improved, and more effective detection, response, and recovery tools and equipment. b. Each organization has established and implemented procedures for periodically updating its business continuity plans and training programs to reflect current ICS detection, response, and recovery tools, equipment, and practices. c. Each organization has developed and implemented employee training programs that provide specialized instruction on the implementation of ICS tools and procedures, and many employees have been trained on these programs, commensurate with their ICS roles and responsibilities. d. Each organization has developed public communication strategies for disseminating the potential transportation network disruption consequences resulting from a cyber incident.
Long-Term (5-10 years)	a. Encourage the widespread implementation and use of automated self-configuring ICS architectures as they become commercially available, in accordance with defined security and safety system priorities. b. Identify and implement real-time detection and response ICS tools and equipment in each mode and throughout the Transportation Sector. c. Research existing ICS cybersecurity certification programs for operators, security, and IT staff, determine which one(s) are best for the organization, and integrate these programs into the organization's overall training/certification program.	a. Self-configuring ICS network architectures are in place in most asset owner/operator facilities, and are in accordance with defined security and safety system priorities. b. Real-time ICS detection and response tools and equipment are present in each mode and throughout the Transportation Sector. c. Many operators, security, and IT staff have successfully completed an ICS cybersecurity certification program that is integrated into the organization's overall training/certification program.
End State:	**The Transportation Sector is quickly alerted of cybersecurity ICS incidents, and sophisticated, effective, and efficient mitigation strategies are implemented and in operation.**	

8.0 Significant Accomplishments

The Transportation Sector has already implemented a variety of proactive cybersecurity programs and initiatives designed to increase awareness on preventing, identifying, and responding to ICS cybersecurity issues. For example, most of the modes have developed, or are in the process of developing, ICS protection standards and procedures. A listing of these standards, along with their current development status, is provided in Appendix C.

One of the long-term objectives described for Goal 1 (Build a Culture of Cybersecurity) in Section 7.0 of this Roadmap is to "establish Information Sharing and Analysis Centers (ISACs) (or equivalent) for each transportation mode and for the Transportation Sector." The purpose of ISACs, or their equivalent, 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. The Surface Transportation Mode already has active ISACs for both surface transportation and public transit. In April 2012, the Aviation SCC official formed an information sharing working group; together with DHS, this group has begun working on the creation of an Aviation ISAC.

9.0 Threats, Challenges, and Priorities

9.1 Threats

Cybersecurity threats in the Transportation Sector have the potential to impact ICSs. For example, new generation aircraft and legacy aircraft are designed or retrofitted with technologies such as Ethernet IP-enabled networks, wireless connectivity (e.g., Bluetooth) capabilities, and GPSs. Similarly, trains are now supplied with onboard IT systems that provide and receive real-time updates on track conditions, train position, train separation, car status, and other operational data. While such technologies are designed to provide faster and more reliable communications, these wireless communication advances result in aircraft and trains no longer functioning as closed systems, thus increasing the e-enabled threats and risks to these transportation mediums.

Many pipelines are now supplied with SCADA systems, RTUs, and automated pressure regulators and control valves. If this pipeline infrastructure is intentionally attacked, many control valves and pressure regulators could simultaneously be affected; if thousands of gas pressure regulators were to fail simultaneously throughout the U.S., the widespread outbreak of pressure surges could cause so many simultaneous explosions and fires that state and local emergency response networks would be overwhelmed, and the resulting conflagrations could destroy entire cities.

Today's control systems in the Highway and Maritime Modes are often not only automated but also highly integrated. Interconnected road networks are controlled by numerous systems and devices such as traffic signal systems, ramp metering systems, road weather information systems, and field devices that feed into a traffic management center. Control systems at ports and terminals not only automate access to particular areas but also control container loading and unloading operations. If an individual system or device was deliberately attacked, the potential to affect multiple control systems would be a distinct reality.

9.2 Challenges

In general, challenges to cybersecurity consist not only of the direct risk factors that increase the probability of a successful attack and the severity of the consequences, but also those factors that limit the ability to implement ideal security enhancements. Risk is defined by threat, vulnerability, and consequences.[28] Direct risk challenges include the threat, i.e., those who seek to attack and compromise cyber system; the means of attack, which relies on taking advantage system vulnerabilities; the nature of the system attacked, such as the degree of hazard of the material; the value of the material and systems; and how loss of control can lead to interaction with humans, property, and the environment. Challenges related to the implementation of security measures include organizational, institutional, economic, and technical factors that either limit the availability of security measures, or increase the difficulty of implementing the optimum security enhancements.[29]

[28] US Department of Commerce, NIST, *Special Publication 800-30: Risk Management Guide for Information Technology Systems*, July 2002.
[29] Chemical Sector Roadmap Working Group, *Roadmap to Secure Control Systems in the Chemical Sector*, September 2009.

9.3 Priorities

Individual ICSs may have inherently different levels of cybersecurity due to modal differences, organizations' business operations, specific policies followed, etc. Under some circumstances, an organization may decide not to activate an ICS cybersecurity feature, based on the organization's risk management assessment/plan, security considerations, or other reasons. Because transportation modes, as well as individual organizations within each mode, are at different stages of identifying and implementing cybersecurity features, a "one size fits all" approach does not work for addressing cybersecurity in the Transportation Sector. Consequently, each organization, and each mode, should use the Goals, Objective, and Milestones and Metrics to identify the cybersecurity features currently in place and to determine the remaining activities necessary for improving cybersecurity performance.

The WG developed this Transportation Roadmap to be a baseline for guiding the transportation industry toward improving ICS cybersecurity. Because the purpose of this Transportation Roadmap is to develop a general 10-year cybersecurity for ICSs outlook that applies to all modes, specificity within each mode and at the individual organization level is not intended for this first roadmap deliverable. As the Transportation Sector matures in ICS cybersecurity and as each mode grows in its cybersecurity knowledge and practices, the Transportation Roadmap should be updated and refined with these additional layers of specificity, including defining specific challenges inherent in securing transportation ICSs, as well as establishing priorities for cybersecurity activity implementation.

10.0 Implementation[30]

This Transportation Roadmap is a living document; it will continue to evolve as the transportation industry reacts to cyber threats, business pressures, operational constraints, societal demands, and unanticipated events. By working together to develop this Transportation Roadmap, the transportation modes have leveraged a broad range of operational and infrastructure protection experience to identify the most significant ICS challenges within the next 10 years and to develop actions that industry and government can take to begin enhancing cybersecurity in the Transportation Sector.

Implementing this Transportation Roadmap will require the continued collective commitment, collaboration, resources, and efforts of the key transportation stakeholders shown in Figure 16. Strong leadership, action, and persistence are needed to ensure that important issues receive adequate support and resources. In addition, achieving early successes and communicating these achievements to the transportation community are important for maintaining momentum generated by the Transportation Roadmap and convincing asset owners and stakeholders that the control systems security framework outlined in this Transportation Roadmap can work.

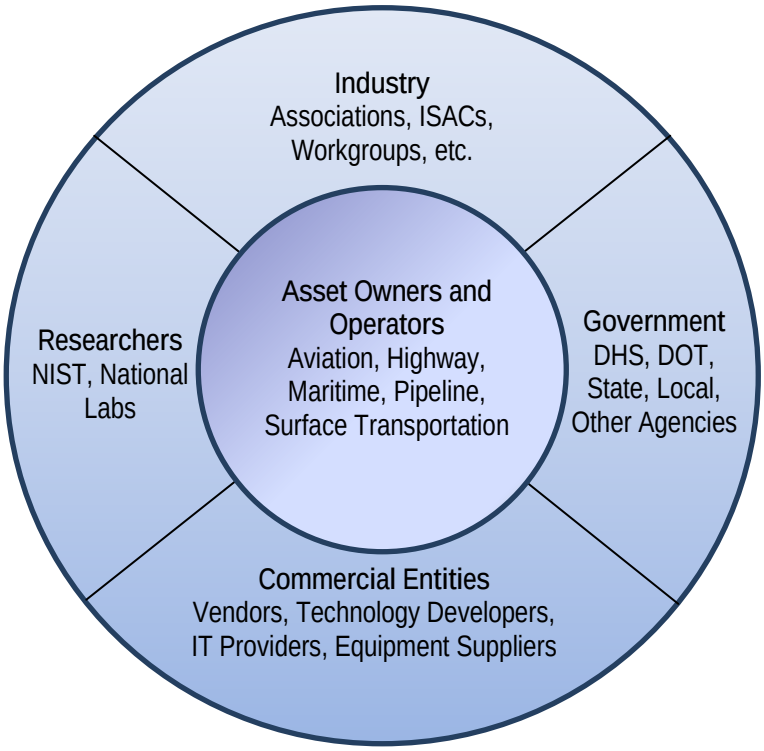

Figure 16: Transportation Stakeholders

[30] Information from the Water Sector Coordinating Council Cyber Security Working Group, *Roadmap to Secure Control Systems in the Water Sector*, March 2008, October 2008, and October 2009 versions, was used to develop this section.

DHS has identified TSA as the SSA for the Transportation Sector and the USCG as the SSA for the Maritime Mode[31]; as such, these agencies are responsible for identifying, prioritizing, and coordinating the protection of CIKR in the Transportation Sector to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them[32]. The U.S. Department of Transportation (DOT) is changed with assisting the Transportation Sector SSAs in their CIKR protection efforts. While the precise roles of organizations in implementing this roadmap have not yet been determined, they will take shape as this Transportation Roadmap is disseminated and reviewed by those engaged. The contributors to this Transportation Roadmap encourage organizations and individuals to participate in ways that will best capitalize on their distinct skills, capabilities, and resources for developing, refining, and expanding on the potential security solutions and enhancements described in the Metrics and Milestones.

Figure 17 identifies the Transportation Roadmap implementation process.

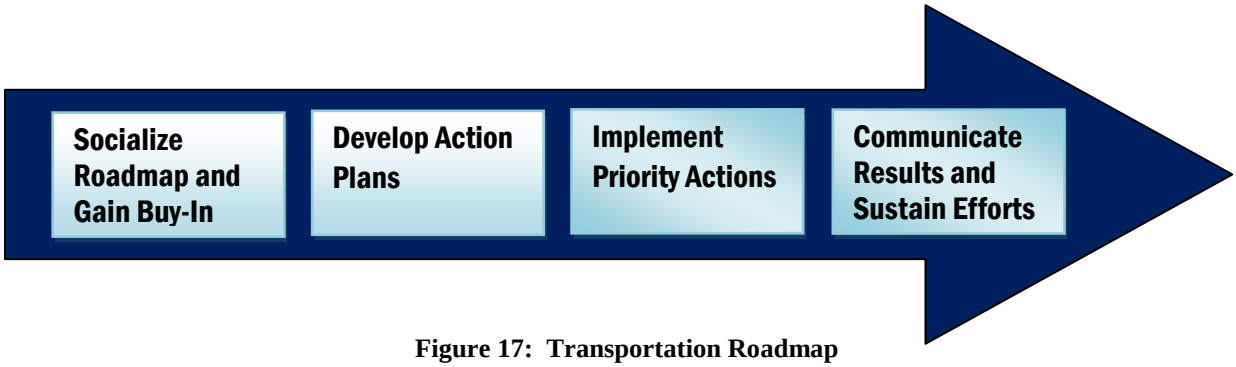

Figure 17: Transportation Roadmap Implementation Process

Socialize Roadmap and Gain Buy-In

While the precise roles of organizations in implementing this Transportation Roadmap have not yet been determined, these roles will take shape as the Transportation Roadmap is disseminated and reviewed by those engaged. The roadmap socialization process should include motivating industry leaders to step forward and initiate the most time-sensitive projects.

Develop Action Plans

Industry and government partners within each transportation mode should collaborate to develop action plans for implementing the Goals and Objectives outlined in this Transportation Roadmap. These action plans should identify a prioritization scheme that reflects those activities deemed most important to protecting the transportation mode's ICS from a cyber attack.

[31] DHS, *Transportation Systems, Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan*, May 2007.
[32] HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection.* December 17, 2003.

Implement Priority Actions
Each transportation mode, and the Transportation Sector as a whole, should execute cybersecurity plans, assess progress, make necessary adjustments, and deliver tangible results. The Milestones and Metrics provided in this Transportation Roadmap provide modal- and Sector-level benchmarks for identifying whether the Objectives have been achieved.

Communicate Results and Sustain Efforts
Each transportation mode should develop a communication strategy that encourages active stakeholder participation within the mode and informs the Transportation Sector on progress. Where possible, transportation modes should utilize/expand on communication capabilities already in place at ISACs and/or the equivalent.

Appendix A: National Policy Guidance on Cyber Control System Security[33]

In 1988, Presidential Decision Directive NSC-63 (PDD-63), "Critical Infrastructure Protection," was issued recognizing the need for enhanced security of the nation's cyber aspects of critical infrastructure. Although directed specifically to information systems, it recognized the interdependencies within the critical infrastructure sectors and the reliance of that infrastructure on automated, cyber systems. The directive called for voluntary private-public partnerships of the type formalized in the NIPP, provided an assignment of government agencies as lead sector agencies, and called for the creation of private sector ISACs, which evolved into the Sector Information Systems Advisory Councils.

Federal Information Security Management Act of 2002 requires that Federal agencies develop a comprehensive information technology security program to ensure the effectiveness of information security controls over information resources that support Federal operations and assets. This legislation is relevant to the part of the NIPP that governs the protection of Federal assets and the implementation of cyber-protective measures under the critical infrastructure Sector-Specific Plans.

The *Cybersecurity Research and Development Act of 2002* allocates funding to the National Institute of Standards and Technology (NIST) and to the National Science Foundation (NSF) for the purpose of facilitating increased R&D for computer network security and supporting research fellowships and training. This act establishes a means of enhancing basic R&D related to improving the cybersecurity of CIKR.

The *National Strategy for Homeland Security* and the *Homeland Security Act of 2002* responded to the attacks of September 11, 2011 by creating the policy framework for addressing homeland security needs and restructuring government activities, which resulted in the creation of DHS.

In early 2003, the *National Strategy to Secure Cyberspace* outlined priorities for protecting against cyber threats and the damage these threats can cause. It called for DHS and the Department of Energy (DOE) to work in partnership 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."

[33] Information from the Industrial Control Systems Cross-Sector Roadmap Working Group, *Cross-Sector Roadmap for Cybersecurity of Control Systems*, September 30. 2011, was used to develop this section.

Appendix A: National Policy Guidance on Cyber Control System Security (continued)

In late 2003, the President issued Homeland Security Presidential Decision 7 (HSPD-7)**,** "Critical Infrastructure Identification, Prioritization, and Protection," to implement Federal policies. HSPD-7 outlined how government will coordinate critical infrastructure protection and assigned DOE the task of working with the Energy Sector to improve physical and cybersecurity in conjunction with DHS. Responsibilities include collaborating with all government agencies and the private sector, facilitating vulnerability assessments of the sector, and encouraging risk management strategies to protect against and mitigate the effects of attacks. HSPD-7 also called for a national plan to implement critical infrastructure protection.

Executive Order (EO) 13231 (as amended by EO 13286 of February 28, 2003 and EO 13385 of September 29, 2005) established the National Infrastructure Advisory Council (NIAC) as the President's principal advisory panel on critical infrastructure protection issues spanning all sectors. The NIAC is composed of not more than 30 President-appointed members, who are selected from the private sector, academia, and state and local government, and represent senior executive leadership expertise from the CIKR as delineated in HSPD-7. The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security—both physical and cyber—of critical infrastructure. The NIAC is charged with improving the cooperation and partnership between the public and private sectors in securing critical infrastructure, and advises on policies and strategies for risk assessment and management, information sharing, and protective strategies and provides clarification on roles and responsibilities between public and private sectors.

Appendix B: Roadmap Process

DHS CSSP and DOT's John A. Volpe National Transportation Systems Center (Volpe Center) signed a Statement of Work agreement in 2011, with one of the major tasks being the development of a roadmap for cybersecurity of control systems in the Transportation Sector (Transportation Roadmap). The Transportation Roadmap specifications were:

- Build upon previous CIKR roadmaps developed to address control systems,
- Utilize key methodology information developed during the creation of the *Cross-Sector Roadmap for Cybersecurity of Control Systems*, and
- Provide a ten-year, high-level outlook and framework for all transportation modes (Aviation, Highway, Maritime, Pipeline, and Surface Transportation—including Freight Rail and Passenger Rail/Public Transit) in the form of cybersecurity control systems goals and milestones.

From March to July 2011, the Volpe Center Roadmap Task Lead conducted a review of the following CIKR roadmaps that were available at the time of the review:

- *Roadmap to Secure Control Systems in the Chemical Sector* (September 2009)
- *Roadmap to Secure Control Systems in the Energy Sector* (January 2006)
- *Roadmap to Secure Control Systems in the Water Sector* (March 2008, October 2008, and October 2009 versions)

In addition, the Volpe Center Transportation Roadmap Task Lead reviewed the *Cross-Sector Roadmap for Cybersecurity of Control Systems* (multiple draft versions, 2011). This roadmap was developed as a guide for CIKR to use to develop sector-specific roadmaps.

The Volpe Center Transportation Roadmap Task Lead compared the four roadmaps; identified the sections and content common to all; identified different sections where similar information was presented; and found common intents among the goals and objectives. These activities culminated in the development of a draft Transportation Roadmap outline and draft Goals, Objectives, Metrics, and Milestones in August 2011.

The Volpe Center Transportation Roadmap Task Lead attended the May 2011 ICSJWG Conference, and participated in the Cross-Sector Roadmap WG meeting held during the conference. Contacts made and information discussed at the meeting provided addition context for developing the Transportation Roadmap.

Appendix B: Roadmap Process (continued)

In July 2011, modal industry and government representatives were invited to participate in a Transportation Roadmap Working Group (WG). Monthly WG teleconference meetings began in August 2011. Because the Goals, Objectives, Metrics, and Milestones information contains the ten-year outlook activities designed to improve transportation control systems cybersecurity, the WG decided to focus its initial efforts on developing this information. From August 2011 to March 2012, the Transportation Roadmap WG reviewed, edited, and added information to the Goals, Objectives, Metrics, and Milestones information, ensuring that the information was applicable to all modes. In April and May 2012, the WG reviewed and developed information for the remaining Transportation Roadmap sections.

The draft Transportation Roadmap was submitted to DHS CSSP for first-level review (initial draft) on May 31, 2012 and for second-level review (final draft) on July 20, 2012.

Appendix C: Transportation Cybersecurity Standards

Mode	Organization	Title	Summary and Additional Information	Status
Aviation	FAA	Information Security Certification and Accreditation (C&A) Handbook	The primary source of procedures and guidance that supports the C&A process in protecting the confidentiality, integrity, and availability of FAA's information that is collected, processed, transmitted, stored, or disseminated in its general support systems, major applications, ICSs, and other applications.	Published
Aviation	RTCA	Airworthiness Security Methods and Considerations	This document is a resource for certification authorities and the aviation industry for developing or modifying aircraft systems and equipment when there is the possibility of danger to flight from volitional human action involving information or information system interfaces. It presents permissible methodologies to meet the data requirements and compliance objectives of an airworthiness security process.	Private Draft
Aviation	RTCA	Airworthiness Security Process Specification	The first of a series of documents on aeronautical systems security that together will address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment. This document addresses only aircraft type certification and is not yet widely implemented, but is derived from understood best practices.	Private Draft
Aviation	AEEC	Guidelines for the Incorporation of Cyber Security in the Development of AEEC Documents	This Technical Application Bulletin represents the current (2009) cyber security thinking and experience useful in the development of further AEEC specifications. The intent is to periodically update the cyber security guidelines and disseminate them to AEEC Subcommittees as conditions warrant.	Under Review
Aviation	ARINC	ARINC Project Paper 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework	The purpose of this document is to facilitate an understanding of aircraft information security and to develop aircraft information security operational concepts. This document also provides an aircraft information security process framework relating to airline operational needs that, when implemented by an airline and its suppliers, will enable the safe and secure dispatch of the aircraft in a timely manner. This framework facilitates development of cost-effective aircraft information security and provides a common language for understanding security needs.	Private Draft

Appendix C: Transportation Cybersecurity Standards (continued)

Maritime	USCG	Command, Control, Communication, Computers and Information Technology (C4IT) Strategic Plan	This plan is intended to be used by the USCG and C4IT community to establish and prioritize recommendations for implementing improvements to the USCG's C4IT infrastructure, systems, applications, products, policies, practices, and processes. The document focuses on activities that must occur in the next five years to begin achieving DHS's and USCG's long-term goals.	Published
Pipeline	INGAA	Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry	This document provides guidance on addressing the control system cybersecurity plans section of the natural gas pipeline operators' TSA-required corporate security program. It provides a set of guidelines to assist operators of natural gas pipelines in managing their control systems cyber security requirements, and sets forth details of the unique risk and impact-based differences between the natural gas pipeline industry and the hazardous liquid pipeline and liquefied natural gas operations.	Published
Pipeline	API	API Standard 1164: Pipeline SCADA Security (Second Edition)	This standard on SCADA security provides guidance to the operators of oil and gas liquid pipeline systems for managing SCADA system integrity and security. The use of this document has applicability beyond pipelines regulated under Title 49 CFR 195.1, and should be viewed as a listing of best practices to be employed when reviewing and developing standards for a SCADA system.	Public Draft
Pipeline	TSA	Pipeline Security Guidelines	These guidelines are applicable to natural gas and hazardous liquid transmission pipelines, natural gas distribution pipelines, and liquefied natural gas facility operators. They also apply to pipeline systems that transport materials categorized as toxic inhalation hazards.	Published
Surface Transportation	APTA	Securing Control and Communications Systems in Transit Environments, Parts 1 and 2	This document addresses the security of the following passenger rail and/or bus systems: SCADA, traction power control, emergency ventilation control, alarms and indications, fire/intrusion detection systems, train control/signaling, fare collection, automatic vehicle location, physical security feeds (CCTV, access control), public information systems, public address systems, and radio/wireless/related communication. In the event that security/safety or other standards exist for any of the above systems, this Recommended Practice will supplement, provide additional guidance for, or provide guidance on how control systems may securely interface with these systems.	Published (Part 1) Final Draft (Part 2)

Appendix D: References

American Public Transportation Association. *Recommended Practice: Securing Control and Communications Systems in Transit Environments--Part 1: Elements, Organization and Risk Assessment/Management*. July 30, 2010.

Chemical Sector Roadmap Working Group. *Roadmap to Secure Control Systems in the Chemical Sector*. Sponsored by the U.S. Department of Homeland Security and the Chemical Sector Coordinating Council. September 2009.

Energetics Incorporated. *Roadmap to Secure Control Systems in the Energy Sector*. Sponsored by the U.S. Department of Energy and the U.S. Department of Homeland Security. January 2006.

Executive Order 13416, *Strengthening Surface Transportation Security*. December 5, 2006.

Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*. December 17, 2003.

Industrial Control Systems Cross-Sector Roadmap Working Group. *Cross-Sector Roadmap for Cybersecurity of Control Systems*. Sponsored by the U.S. Department of Homeland Security. September 30. 2011.

Presidential Decision Directive NSC-63, *Critical Infrastructure Protection*. May 22, 1998.

United States Code, Title 44, Section 301, *Federal Information Security Management Act of 2002*.

U.S. Department of Commerce, National Institute of Standards and Technology. *Special Publication 800-53A: Guide for Assessing the Security Controls in Federal Information Systems and Organizations*. Revision 1. June 2010.

U.S. Department of Commerce, National Institute of Standards and Technology. *Special Publication 800-30: Risk Management Guide for Information Technology Systems*. July 2002.

U.S. Department of Commerce, National Institute of Standards and Technology. *Special Publication 800-82: Guide to Industrial Control Systems Security*. June 2011.

U.S. Department of Homeland Security. *National Cyber Security Division Style Guide*. February 2012.

U.S. Department of Homeland Security. *National Infrastructure Protection Plan*. 2009.

U.S. Department of Homeland Security. *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*. October 2009.

Appendix D: References (continued)

U.S. Department of Homeland Security. *Strategy for Securing Control Systems: Coordinating and Guiding Federal, State and Private Sector Initiatives*. October 2009.

U.S. Department of Homeland Security. *Transportation Systems: Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan*. May 2007.

U.S. Department of Homeland Security. *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*. 2010.

U.S. Department of Homeland Security, National Protection and Programs Directorate. *Enabling Distributed Security in Cyberspace*. March 23, 2011.

Water Sector Coordinating Council Cyber Security Working Group. *Roadmap to Secure Control Systems in the Water Sector*. Sponsored by the U.S. Department of Homeland Security and the American Water Works Association. March 2008, October 2008, and October 2009 Versions.

White House Release. *The Comprehensive National Cybersecurity Initiative*. March 2, 2010.

White House Release. *National Strategy for Trusted Identities in Cyberspace*. April 2011.

Appendix E: Acronyms

AEEC	Airlines Electronic Engineering Committee
AFDX	Avionics Full Duplex Switched Ethernet
API	American Petroleum Institute
APTA	American Public Transportation Association
ARINC	Aeronautical Radio, Incorporated
ATIS	Advanced traveler Information System
CCTV	Closed Circuit Television
CIKR	Critical infrastructure and Key Resources
COTS	Commercial Off-the-Shelf
CSET	Cybersecurity Evaluation Tool
CSSP	Control Systems Security Program (DHS)
DCS	Distributed Control System
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOT	Department of Transportation
ECP	Electronically Controlled Pneumatic (brakes)
EFB	Electronic Flight Bag
EO	Executive Order
FAA	Federal Aviation Administration
GCC	Government Coordinating Council
GPC	General-Purpose Controller
GPS	Global Positioning System
HMI	Human-Machine Interface
HSPD	Homeland Security Presidential Directive
HUMS	Health and Usage Monitoring System
HVAC	Heating, Ventilation, and Air Conditioning
ICS	Industrial Control System
ICSJWG	Industrial Control Systems Joint Working Group

Appendix E: Acronyms (continued)

INGAA	Interstate Natural Gas Association of America
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
ITS	Intelligent Transportation Systems
LAN	Local Area Network
NAS	National Airspace System
NCSD	National Cybersecurity Division (DHS)
NIAC	National Infrastructure Advisory Council
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
PID	Passenger Information Display
PLC	Programmable Logic Controller
PTC	Positive Train Control
R&D	Research and Development
RTCA	Radio Technical Commission for Aeronautics
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SSA	Sector-Specific Agency
TEU	Twenty-foot Equivalent Unit
TSA	Transportation Security Administration
USCG	United States Coast Guard
VTS	Vessel Traffic Service
VTC	Vessel Traffic Center
WAN	Wide Area Network
WLAN	Wireless Local Area Network