2013-2023

Transportation Industrial Control Systems (ICS) Cybersecurity Standards Strategy

Lisa Kaiser (ICS-CERT)

U.S. Department of Homeland Security

(This Page Intentionally Blank)

Executive Summary

Industrial Control Systems (ICS) manage, command, direct, or regulate the behavior of other devices or systems used in industrial production. All transportation modes: highway, surface transportation, aviation, maritime, and pipeline are becoming increasingly dependent on these devices to perform operational and safety-critical functions. The Department of Homeland Security (DHS) Control Systems Security Program (CSSP) recommends standardizing transportation ICS cybersecurity practices because of the widespread use of ICS and the economic and social impacts of a transportation cyber-event. ICS cybersecurity is a fledgling concern in the transportation sector, and preliminary research has illustrated that while some modes have developed relevant standards, most of them have failed to address ICS cybersecurity. This document identifies short and long-term goals to address these gaps in ICS cybersecurity standards, and outlines the estimated cost, timeline, and deliverables associated with meeting those goals.

The Highway mode of transportation includes thousands of miles of highway and the vehicles that operate on them. Highway is the mode of transportation furthest behind in transportation ICS cybersecurity standard development. In the short term, we will engage standards development organizations (SDOs) and federal agencies to create a highway ICS working group. The focus of the group will be identifying and classifying common highway ICS systems. In the long term, SDOs will use the classification document to create a full-fledged highway ICS cybersecurity standard.

The Maritime mode includes all ports, vessels, and inland waterways in and surrounding the United States. We will work with maritime regulatory bodies to identify common maritime ICS systems. Initially, the focus will be on classifying and identifying vessel ICS; in the long-term port ICS systems will be addressed. These classification documents serve as the basis for future vessel and port ICS cybersecurity standards.

The Aviation mode includes all aircraft and airports in the United States, and is among the most advanced of the modes when it comes to Control System (CS) cybersecurity standards. Existing standards have focused on aircraft CS but have not directed attention to airports. We will address this inconsistency by working with airports to identify and classify common airport CS. Much like the other modes, the intent of this classification is to create an airport CS cybersecurity standard.

The Surface Transportation mode includes public transit systems and freight rail in the United States. The mode is on the right track in terms of standards development and has addressed public transit systems, but the freight rail industry has not created a cybersecurity standard. In the short term, we will work to review transit ICS cybersecurity standards, and work with freight rail operators to identify ICS cyber evaluation metrics. In the long term, we will work toward extending the transit ICS cybersecurity standard to include intrabuses. Trucking and intercity bus service, as well as the freight rail industry, may use the metrics to develop ICS cybersecurity standards specific for their industry.

The Pipeline mode is the most advanced in terms of ICS cybersecurity. There are numerous regulatory standards addressing ICS cybersecurity within the mode, and outreach with the organizations contacted has yielded little traction. We will focus its efforts on the other modes since ICS cybersecurity standards are progressing well in the Pipeline mode.

Contents

1 Introduction

The Department of Homeland Security (DHS) National Cyber Security Division (NCSD) is working across the government, collaborating with the private sector, and empowering the public to create a safe, secure, and resilient cyber environment, and to promote cybersecurity knowledge and innovation. Homeland Security Presidential Directive-7 established U.S. policy for identifying, prioritizing, and protecting the Nation's eighteen critical infrastructure/key resources (CI/KR) from terrorist attacks. The NCSD's Control Systems Security Program (CSSP) mission is to reduce risk to the Nation's critical infrastructure by strengthening control systems security through public-private partnerships. This Plan focuses on how the U.S. DHS CSSP will advance industrial control system (ICS) cybersecurity standards development in the Transportation sector over the next five years.

1.1 Background

This section summarizes the five transportation modes, and identifies current ICS cybersecurity standards and their purpose, in addition to areas of improvement for cybersecurity standards.

1.1.1 Highway

The Highway mode covers thousands of miles of highways and the vehicles that operate on them. The Volpe Center researched the activities of the U.S. DOT Federal Highway Administration (FHWA) and National Highway Traffic Safety Administration (NHTSA), in addition to SDOs, including the Society of Automotive Engineers (SAE) and the American Association of State Highway and Transportation Officials (AASHTO).

DOT and these SDOs are not actively developing control systems cybersecurity standards at this time. Among the five modes, Highway has the fewest number of ICS cybersecurity standards initiatives.

1.1.2 Maritime

The Maritime mode covers all ports, vessels, and inland waterways in and surrounding the United States. The major governing body and standards organization is the U.S. Coast Guard (USCG). Currently no standards exist to address the numerous control systems located in ports, terminals, and onboard vessels. The USCG Cyber Command (USCG-CC) recognized the need for sound cybersecurity policy, and created the Command, Control, Communication, Computers, and Information Technology (C4&IT) Strategic Plan. We recommend that the USCG have a role in creating cybersecurity standards.

1.1.3 Aviation

The Aviation mode covers all aircraft and airports in the United States. Compared with the other Transportation modes, it is one of the most advanced in its use of cybersecurity standards. Over the past few years the Airlines Electronic Engineering Committee (AEEC) and the Aircraft Information Security subcommittee have been working with several American and international organizations, including the Radio Technical Commission for Aeronautics (RTCA), Aeronautical Radio Incorporated (ARINC), and the European Organization for Civil Aviation Equipment (EUROCAE). Together, these organizations have produced several documents,

unavailable to the public at this time, to promote the implementation of cybersecurity standards in the aviation industry.

RTCA's Aeronautical Systems Security Sub Committee 216 (SC-216) and EUROCAE Working Group 72 (WG-72) jointly drafted *Airworthiness Security Methods and Considerations* in August 2010. This document remains a rough draft; its purpose is to ensure that future aircraft will be able to fly despite the potential misuse of aircraft information systems due to a variety of technical issues ranging from malware infection, denial of service, and unauthorized access, to safety-critical systems and interfaces. RTCA intends this document to be used "as a resource for certification authorities and the aviation industry for developing or modifying aircraft systems and equipment when there is the possibility of a danger to flight from volitional human action involving information or information system interfaces."[1]

The same group published *Airworthiness Security Process Specification* in October, 2010. This document focuses on the same major areas as the *Airworthiness Security Methods and Considerations*. The major difference is that the Specification document describes a lifecycle process for aircraft system security in partnership with existing industry best practices. It also provides compliance objectives organized by generic activities for aircraft development in order to ensure that aircraft are not only safe, but also secure.

The Aviation mode has made great strides in securing CS for aircraft; however, cybersecurity standards have not addressed CS in airports.

1.1.4 Surface Transportation

The Surface Transportation mode covers public transit systems and freight rail in the United States. This mode is on the right track with ICS cybersecurity standards development for public transit systems but the freight rail industry does not have a cybersecurity standard.

The American Public Transit Association (APTA) has had a major role in advancing transportation ICS cybersecurity standards with the publication of its recommended practice, *Securing Control and Communications Systems in Transit Environments, Part 1: Elements, Organization and Risk Assessment/Management*, in July 2010. It focuses on elements, organization, and risk assessment/management of ICS systems in public transportation. *Securing Control and Communications Systems in Transit Environments, Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones* should be published at the end of 2012 or beginning of 2013. These two standards are good starting points in defining a comprehensive cybersecurity standard for the United States' public transit infrastructure.

1.1.5 Pipeline

The Pipeline mode has published several relevant ICS cybersecurity standards. Major industry players include the American Petroleum Institute (API), Interstate Natural Gas Association of America (INGAA), and Transportation Safety Administration (TSA).

[1] RTCA Aeronautical Systems Security Sub-Committee 216 (SC-216) and EUROCAE Working Group 72 (WG-72), FAA Airworthiness Security Methods and Considerations, p. 11, August 2010.

API released the first standard, *API Standard 1164: Pipeline SCADA Security*, in June, 2009. The standard provides owners and operators of oil and gas liquid pipelines with guidance on maintaining Supervisory Control and Data Acquisition (SCADA) control systems and provides a framework to ensure industry best practices for SCADA system security. The goal of the standard is to help pipeline owner/operators build in security as part of a new deployment or lifecycle upgrade instead of viewing security as a last-minute fix. It presents a high-level view of all-inclusive security practices, with more detailed technical guidance in the appendices.

INGAA's Control Systems Cybersecurity Working group released *Control Systems Cybersecurity Guidelines for the Natural Gas Pipeline Industry* in January, 2011. The purpose of the document is to "provide guidance on addressing the control system cybersecurity. It is a set of guidelines to assist operators of natural gas pipelines in managing their control systems cybersecurity requirements. It sets forth and details the unique risk and impact-based differences between the natural gas pipeline industry, hazardous pipeline and liquefied natural gas operators."[2]

The INGAA standard is similar to the TSA *Pipeline Security Guidelines*. TSA developed its guidelines with input from government and private industry in order to address growing security concerns following the events of 9/11. These guidelines are at a much less technical level than the other pipeline standards. Topics covered include creating a corporate security plan, risk analysis, criticality criteria, facility security, and cyber asset security measures..

1.2 Vision

In maintaining alignment with the DHS Control Systems Security Program (CSSP), the vision is *control systems security activities for critical infrastructures/key resources will be successfully coordinated across all sectors to effectively manage risk.*

1.3 Scope

There are five main components to the Transportation ICS Cybersecurity Standards Strategy:

- Complete a list of existing ICS cybersecurity standards for each mode.
- Perform a gap analysis of existing transportation ICS cybersecurity standards by mode to identify lags in standards development.
- Define short-term (one and two year) and long-term (three-to-five year) goals and objectives for transportation cybersecurity standards development within each mode.

1.4 Assumptions and Constraints

The following assumptions are in place:

- Participation from transportation standards development organizations (SDOs) within each mode,

[2] INGAA, Control Systems Cybersecurity Working Group, Control Systems Cybersecurity Guidelines for the Natural Gas Pipeline Industry, p.2, January 2011.

- Volunteers from each mode with adequate expertise to add standards development value to the process,
- Engagement from participants that is active and supportive of the effort through completion, and
- Consensus from all participants on cybersecurity standards for adoption.

The following constraints are in place:

- Lax in participation from external organizations, including SDOs,
- Reluctance of each mode to develop ICS cybersecurity standards,
- Inability to adequately identify transportation ICS critical infrastructure within modes,
- Narrow SME knowledge of the interrelationship between transportation ICS and cybersecurity,
- Exclusion of non-ICS transportation systems and standards, and
  Restrictions in budget and resources

1.5 Authority

This Transportation Industrial Control System (ICS) Cybersecurity Standards Strategy relies on the authority of several strategies, plans, and advisories (reference Figure 1) since 2003 that shape the U.S. Federal activities in support of improving control systems cybersecurity.

The latest publication is an initial public draft (IPD) of a *Roadmap to Secure Control Systems in the Transportation Sector*[3] that is presently out for public review and comment. This document addresses the short and long term goals and objectives for cybersecurity within transportation control systems. This strategy must align with the final version so additional edits may be forthcoming.

[3] Roadmap to Secure Control Systems in the Transportation Sector, p.33, IPD August 2012 (http://www.us-cert.gov/control_systems/pdf/TransportationRoadmap083112.pdf).

Document	Author	Release Date	Type	Summary
National Strategy to Secure Cyberspace	Presidential Directive	2003	Policy	Provides policy direction to DHS and federal agencies on cybersecurity, including control systems. Identifies DHS as the lead agency in this effort.
HSPD-7	Presidential Directive	2003	Policy	DHS, in coordination with other sector-specific agencies, to prepare a national plan to protect the infrastructure to include coordination and participation with the private sector.
Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems	GAO	2004	Advisory	Recommends DHS develop and implement a strategy to coordinate efforts to meet challenges associated with securing control systems and current efforts for both the federal and private sector.
National Infrastructure Protection Plan	DHS	2006	Plan	Provides the overarching planning process and structure for security partnerships and federal/private sector response to protect critical infrastructure.
Sector Specific Plans	SSA	2007	Plan	All Sector Specific Agencies (SSAs) in coordination with SCCs were directed to complete plans within the NIPP partnership framework by 2006. These provide high level assessment, goals, and objectives for infrastructure protection.
Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain	GAO	2007	Advisory	Recommends DHS develop a coordination strategy for public and private sectors and process for improving information sharing.
Academic: • Toward a Safer and More Secure Cyberspace	NRC	2007	Advisory	The National Research Council (NRC) conducted a study on research priorities for securing cyberspace. Control systems issues were included in their scope.
Sector-Specific Roadmaps/Strategies: • Energy Sector Roadmap • Nuclear Sector Roadmap • Guidance for Addressing Cyber Security in the Chemical Industry • Water Sector Roadmap • Cross-Sector Roadmap • IPD Transportation Sector Roadmap	DOE/SCC ACC/SCC DHS/SCC DHS/SCC	2006 2006 2008 2012 2012	Plan	Roadmaps provide detailed assessment of where the sector currently stands on initiatives for cybersecurity of control systems, and a plan for reaching an end state that provides for prevention, detection, and mitigation of attacks on these systems.
NSPD-54/HSPD-23	Presidential Directive	2008	Policy	Mandatory intrusion detection requirements for federal facilities.

Figure 1 – Timeline of policy, advisories, and plans supporting control systems cybersecurity

1.6 Alignment with DHS and NPPD Goals

This CSSP strategy for transportation standards aligns with corresponding DHS and National Program and Protections Directorate (NPPD) standards for consistency (reference Figure 2).

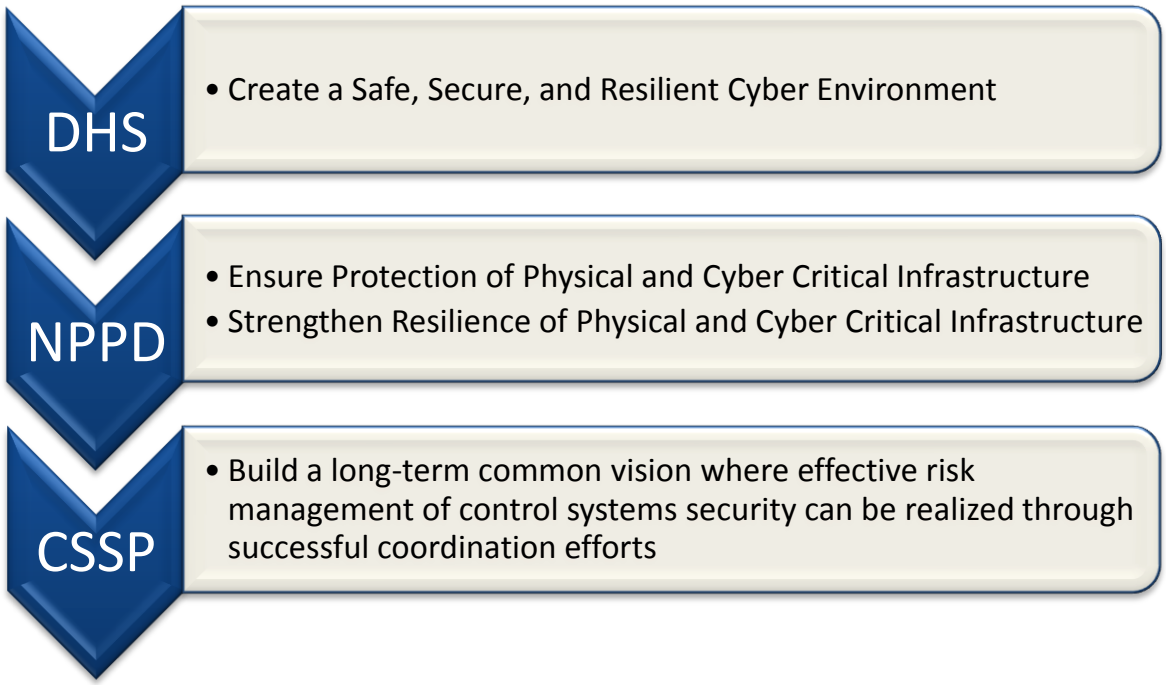

Figure 2 – Strategy Alignment with Goals

2 Goals for Transportation Cybersecurity

This section outlines the short and mid-term goals and milestones for cybersecurity standards for transportation control systems. The timeline to complete all these goals is five years ending in December 2018. Figure 3 provides an illustration of these goals and milestones by mode.

SHORT-TERM GOALS				
Aviation	***Highway***	***Maritime***	***Pipeline***	***Surface Transportation***
• Identify and classify common airport ICS systems. • Brief ACI-NA BIT group on findings.	• Form a highway ICS cybersecurity standards working group with FHWA, NHTSA, AASHTO and SAE. • Classify and identify common highway ICS systems.	• Form a Vessel ICS cybersecurity standards working group. • Classify and identify common vessel ICS systems.	• Focus on API and INGAA standards development enhancements.	• Review APTA standard Securing Control and Communications Systems in Transit Environments. • Engage Class I rail operators to compile cyber evaluation metrics. • Continue to support the APTA-Control and Communications Cyber Security Work Group.
MID-TERM GOALS				
Aviation	***Highway***	***Maritime***	***Pipeline***	***Surface Transportation***
• Identify SDO to lead airport ICS cybersecurity standard effort. • Create Airport ICS cybersecurity standard.	• Create Highway ICS cybersecurity standard.	• Form a Port ICS Cybersecurity Standard Working group. • Participate in Vessel and Port ICS Cybersecurity Standard Working groups. • Identify and classify common port ICS systems. • Create Vessel and Port ICS cybersecurity standard.	• Focus on API and INGAA standards development enhancements.	• Extend APTA ICS standard to buses and trucks. • Create freight rail ICS cybersecurity standard working group. • Create freight rail ICS cybersecurity standard.
MILESTONES				
Aviation	***Highway***	***Maritime***	***Pipeline***	***Surface Transportation***
• Final version airport ICS cybersecurity standard	• Final version highway ICS cybersecurity standard	• Final version vessel ICS Cybersecurity standard • Final version port ICS standard	• Revision to API and INGAA standards.	• Updated APTA standard • Final version freight rail ICS cybersecurity standard

Figure – Transportation Cybersecurity Standards Goals and Milestones by Mode

2.1 Short-Term Goals by Mode

This section outlines the short-term goals for each mode of transportation. The timeline to complete these goals is two years, beginning in January, 2013 and ending in December, 2014.

2.1.1 Highway

The Highway mode is the furthest behind in developing ICS cybersecurity standards. On behalf of DHS CSSP, we will network with highway mode SDOs to raise awareness about ICS cybersecurity. To meet this goal, we will form a working group with members from FHWA, NHTSA, AASHTO and SAE. By networking with these organizations, DHS CSSP will identify common ICS in highways and vehicles and create transportation ICS cybersecurity standards addressing all aspects of the highway mode.

Short-term Goal 1: Form a highway ICS cybersecurity standards working group with FHWA, NHTSA, AASHTO and SAE.
Short-term Goal 2: Classify and identify common highway ICS systems.
Milestone: Highway ICS classification document

2.1.2 Maritime

Maritime is similar to other transportation modes since it does not adequately address ICS cybersecurity standards. The difference is that the USCG-CC recently published the C4&IT Strategic Plan outlining the need for cybersecurity standards. USCG-CC is an important partner for CSSP and will be the main contact for maritime standards development over the next few years.

When breaking down the maritime mode it is important to note the difference between port and vessel regulation. Creating ICS standards for ports is more difficult due to their complex and inconsistent behavior over regulation. In the short term, we will focus on vessel regulation.

We will form a vessel ICS cybersecurity working group to address vessel regulation. The working group will include members from the Maritime Administration (MARAD), USCG-CC, and the American Bureau of Shipping (ABS). Its focus will be to identify common control systems and best practices to ensure that ICS design and implementation on new and existing vessels is secure.

Short-term Goal 1: Form a Vessel ICS cybersecurity standards working group.
Short-term Goal 2: Classify and identify common vessel ICS systems.
Milestone 1: Maritime ICS classification document

2.1.3 Aviation

The Aviation mode understands the need for ICS cybersecurity standards. Several standards addressing ICS cybersecurity of airborne vehicles are currently under review. These reviews should conclude before 2013; they do not address airport ICS cybersecurity.

Airport ICS cybersecurity is a new concept. In the short term, we will work with the Airport Council International – North America (ACI-NA) Business Information Technology (BIT) group to develop airport ICS cybersecurity standards. We will also work with ACI-NA and with major and minor airports in compiling common control systems and best practices for airport ICS cybersecurity. The document will detail types of systems required and will be a good first step towards standardizing airport ICS.

Short-term Goal 1: Identify and classify common airport ICS systems.
Short-term Goal 2: Engage with ACI-NA BIT group on findings.
Milestone 1: Aviation Classification document

2.1.4 Surface Transportation

ICS cybersecurity for Surface Transportation falls into two groups: public transit and freight rail. Public transit is farther ahead of freight rail in developing ICS cybersecurity standards. In the short term, we will review these standards and compare them to existing CSSP best practices.

Larger surface transportation organizations, including Class I rail operators, have not addressed ICS cybersecurity standards. Traditionally, these infrastructure operators are resistant to federal regulation. CSX Corporation, a major outreach partner with CSSP-Transportation, is willing to formulate "cyber evaluation metrics," which could be used as a baseline for an ICS standard. In the short term, we will engage CSX and other Class I rail operators through the American Association of Railroads (AAR) to compile and publish the cyber evaluation metrics.

Short-term Goal 1: Review APTA standard *Securing Control and Communications Systems in Transit Environments.*
Short-term Goal 2: Engage Class I rail operators to assist with obtaining cyber evaluation metrics.
Short-term Goal 3: Continue to support the APTA-Control and Communications Cyber Security Work Group.
Milestone 1: Class I Cyber Evaluation Metrics

2.1.5 Pipeline

The Pipeline mode is the most advanced in developing ICS cybersecurity standards. Outreach with the pipeline organizations has taught us that these operators rely heavily on API standards. We will continue to focus on API and standards development but will focus more on working with the other four modes in developing standards.

Short-term Goal 1: Focus on API and INGAA standards development enhancements.

2.2 Mid-Term Goals by Mode

This section outlines the long-term goals for each transportation mode. The timeline to complete these goals is three to five years, beginning in, 2013 and ending in December, 2018.

2.2.1 Highway

Developing a Highway ICS cybersecurity standard is the long-term goal for the Highway mode. We will follow up with the highway ICS cybersecurity standards working group made up of NHTSA, FHWA, AASHTO, and SAE. The group will select an appropriate SDO to draft, review, and publish highway ICS cybersecurity standards. The working group will use its earlier Highway ICS Classification document as a baseline for the standard.

Mid-term Goal 1: Create Draft and Final Highway ICS cybersecurity standard.
Milestone 1: Complete final version Highway ICS cybersecurity standard

2.2.2 Maritime

Expanding vessel ICS cybersecurity standards and working with ports is the long-term goal for the Maritime mode. By participating in the vessel ICS cybersecurity standards working group, we can identify an appropriate SDO to draft, review, and finalize a comprehensive vessel ICS cybersecurity standard.

We can follow a similar process with ports. By leveraging lessons learned from the vessel standards working group, we will create a port ICS cybersecurity standards working group. This group will include members from the American Association of Port Authorities (AAPA) and regional port authorities and will focus on identifying and classifying common control systems and best practices at ports. This classification will be the baseline for a port ICS cybersecurity standard. The draft and review process will be the same as for the vessel standard.

Mid-term Goal 1: Form a Port ICS Cybersecurity Standard Working group.
Mid-term Goal 2: Identify and classify common port ICS systems.
Mid-term Goal 3: Create Vessel and Port ICS cybersecurity standard.
Milestone 1:Complete final version of vessel and port ICS cybersecurity standards

2.2.3 Aviation

Generating an airport CS cybersecurity standard is the long-term focus for the Aviation mode. We will work with the ACI-NA BIT group, the FAA, and other partners to identify and select an appropriate SDO. The SDO will be responsible for drafting, reviewing, and publishing an Airport ICS cybersecurity standard.

Mid-term Goal 1: Identify SDO to lead airport ICS cybersecurity standard effort.
Mid-term Goal 2: Create draft and final airport ICS cybersecurity standard.
Milestone 1:Complete final version airport ICS cybersecurity standard

2.2.4 Surface Transportation

Expanding the APTA ICS standard to include buses and trucks and creating a working group focused on freight rail ICS cybersecurity are the long-term goals for the Surface Transportation mode. We will work with the freight rail industry to create this working group. Cyber

evaluation metrics will be used as a baseline to develop an overarching freight rail ICS cybersecurity standard.

Mid-term Goal 1: Complete extension of APTA ICS standard to buses and trucks.
Mid-term Goal 2: Create freight rail ICS cybersecurity standard working group.
Mid-term Goal 3: Create freight rail ICS cybersecurity standard.
Milestone 1: Complete update to APTA standard and final version freight rail ICS cybersecurity standard

2.2.5 Pipeline

Long-term goals for the Pipeline mode are the same as the short-term goals. We will stay abreast of API standards development and will focus efforts on working with the other four modes in developing standards.

Mid-term Goal 1: Focus on API and INGAA standards development enhancements.
Milestone 1: Complete revision to API and INGAA standards.

3 Strategic Concepts by Mode

This section provides an overview of tasks, deliverables, and estimated costs between 2013 and 2017, broken down by mode.

3.1 Highway

Year	2013	2014	2015	2016	2017
Tasks	Engage NHTSA, SAE, AASHTO, and FHWA to form a highway ICS cybersecurity standards working group	Identify and classify highway and automotive ICS systems	Write highway ICS cybersecurity standard draft	Review highway ICS cybersecurity standard	Publish highway ICS cybersecurity standard final draft
Deliverables	Meeting attendance, agendas, and minutes	Highway ICS Classification document	Draft Highway ICS Cybersecurity Standard	Revision history of Highway ICS Cybersecurity Standard	Final Draft Highway ICS Cybersecurity Standard

3.2 Maritime

Year	2013	2014	2015	2016	2017
Tasks	Engage MARAD, USCG-CC, & ABS to form a Vessel ICS cybersecurity standards working group	Identify and classify Vessel ICS systems	Write Vessel ICS cybersecurity standard draft Engage AAPA and regional port authorities to form Port ICS cybersecurity working group	Review Vessel ICS cybersecurity standard Identify and classify Port ICS systems	Publish Vessel ICS cybersecurity standard draft
Deliverables	Meeting attendance, agendas, and minutes	Vessel ICS Classification document	Draft Vessel ICS Cybersecurity Standard	Revision history of Vessel ICS Cybersecurity Standard Port ICS Classification document	Final Draft Vessel ICS Cybersecurity Standard Draft Port ICS Cybersecurity Standard

3.3 Aviation

Year	2013	2014	2015	2016	2017
Tasks	Engage ACI-NA BIT group and airports around the country to form airport ICS working group	Identify and classify Airport ICS systems Brief working group on findings	Research Aviation SDOs Write Airport ICS cybersecurity standard draft	Review Airport ICS cybersecurity standard	Publish Airport ICS cybersecurity standard final draft
Deliverables	Meeting attendance, agendas, and minutes	Airport ICS Classification document ACI-NA BIT group findings	SDO Decision Justification Draft Airport ICS Cybersecurity Standard	Revision history of Airport ICS Cybersecurity Standard	Final Draft Airport ICS Cybersecurity Standard

3.4 Surface Transportation

Year	2013	2014	2015	2016	2017
Tasks	Review APTA standard Engage Class I operators to form Class I Rail ICS working group	Remain involved with APTA standard working group Compile cyber evaluation metrics for Class I operators	Write APTA ICS cybersecurity standard draft for buses and trucks Write freight rail ICS cybersecurity standard draft	Review APTA ICS cybersecurity standard for buses and trucks Review Freight Rail ICS cybersecurity standard	Publish Buses and Trucks ICS cybersecurity standard Publish Freight Rail ICS cybersecurity standard
Deliverables	APTA revisions Meeting attendance, agendas, and minutes	APTA working group minutes cyber evaluation metrics	Draft Buses and Trucks ICS cybersecurity Standard Draft Freight Rail ICS cybersecurity Standard	Revision history of Buses and Trucks ICS cybersecurity standard Revision history of Freight Rail ICS cybersecurity standard	Final Draft Buses and Trucks ICS cybersecurity Standard Final Draft Freight Rail ICS cybersecurity Standard

Appendix A - Acronyms

AAPA	American Association of Port Authorities
AAR	American Association of Railroads
AASHTO	American Association of State Highway and Transportation Officials
ABS	American Bureau of Shipping
AEEC	Airlines Electronic Engineering Committee
API	American Petroleum Institute
APTA	American Public Transportation Association
ARINC	Aeronautical Radio Incorporated
CSSP	Control Systems Security Program
EUROCAE	European Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration, US Department of Transportation
FHWA	Federal Highway Administration, US Department of Transportation
FTA	Federal Transit Administration
ICS	Industrial Control System(s)
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
INGAA	Interstate Natural Gas Association of America
MARAD	Maritime Administration, US Department of Transportation
NHTSA	National Highway Traffic Safety Administration, US Department of Transportation
PHMSA	Pipeline and Hazardous Materials Safety Administration, US DOT
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automotive Engineers
SCADA	Supervisory Control and Data Acquisition
SDO	Standards Development Organization
U.S. DHS	United States Department of Homeland Security
U.S. DOT	United States Department of Transportation
USCG-CC	United States Coast Guard – Cyber Command

Appendix B – Transportation ICS Cybersecurity Standards Summary

Standards					
Organization	**Mode**	**Title**	**Description**	**Status, Date, Cost**	**URL**
FAA	Aviation & Aerospace	Information Security Certification and Accreditation (C&A) Handbook	Primary source of procedures and guidance that support the C&A Process in protecting the confidentiality, integrity, and availability of the FAA's information collected, processed, transmitted, stored, or disseminated in its general support systems (GSS), major applications (MA), industrial control systems (ICS), and other applications.	Published 2010, free	faaco.faa.gov/attachments/C_A_Handbook_060509.doc
RTCA	Aviation & Aerospace	Airworthiness Security Methods and Considerations	Resource for certification authorities and the aviation industry for developing or modifying aircraft systems and equipment when there is the possibility of a danger to flight from volitional human action involving information or information system interfaces. Presents permissible methodologies to meet the data requirements and compliance objectives of an airworthiness security process.	Private Draft	Closed to public
RTCA	Aviation & Aerospace	Airworthiness Security Process Specification	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. Addresses only Aircraft Type Certification and is not yet widely implemented, but is derived from understood best practice.	Private Draft	Closed to Public
AEEC	Aviation & Aerospace	Guidelines for the incorporation of Cyber Security in the Development of AEEC Documents	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 it to AEEC Subcommittees as conditions warrant.	Under Review	Closed to public

Standards					
Organization	**Mode**	**Title**	**Description**	**Status, Date, Cost**	**URL**
ARINC	Aviation & Aerospace	ARINC Project Paper 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework	Facilitates an understanding of aircraft information security and develops aircraft information security operational concepts. This common understanding is important since a number of subcommittees and working groups within the aeronautical industry are considering aircraft information security. 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.	Published 2005, $356	https://www.arinc.com/cf/store/catalog_detail.cfm?item_id=617
USCG-CC	Maritime	Command, Control, Communication, Computers and Information Technology (C4IT) Strategic Plan	For members of the C4IT community and Coast Guard to establish and prioritize recommendations for implementing improvements to the Coast Guard's C4IT infrastructure, systems, applications, products, policies, practices, and processes. The focus of this document is on activities that must occur in the next five years to begin achieving the long-term goals of the Coast Guard and the Department of Homeland Security (DHS).	Published 2010	http://www.uscg.mil/hq/cg6/docs/C4IT_Strategic_Plan_FY11-15.pdf
INGAA	Pipeline	Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry	Provides guidance on addressing the control system cyber security plans section of the natural gas pipeline operators' TSA-required CSP. It is a set of guidelines to assist operators of natural gas pipelines in managing their control systems cyber security requirements. It sets forth and details the unique risk and impact-based differences between the natural gas pipeline industry and the hazardous liquid pipeline and liquefied natural gas operators referenced equally in the aforementioned TSA guidelines.	Published January, 2011 Free	http://www.aga.org/membercenter/gotocommitteepages/NGS/Documents/INGAAControlSystemsCyberSecurityGuidelines.pdf
API	Pipeline	API Standard 1164	Provides guidance to the operators of oil and gas liquids pipeline systems for managing SCADA system integrity and security. The use	Second Edition	http://www.techstreet.com/standards/api/std_1164?product_i

Standards					
Organization	**Mode**	**Title**	**Description**	**Status, Date, Cost**	**URL**
		Pipeline SCADA Security, Second Edition	of this document is not limited to pipelines regulated under Title 49 CFR 195.1, but should be viewed as a listing of best practices to be employed when reviewing and developing standards for a SCADA System.	published June 2009, $141	d=1629005
TSA	Pipeline	Pipeline Security Guidelines	Applicable to natural gas and hazardous liquid transmission pipelines, natural gas distribution pipelines, and to liquefied natural gas facility operators. Additionally they apply to pipeline systems that transport materials categorized as toxic inhalation hazards (TIH).	Published December 2010 Free	http://www.ilta.org/WhatsNew/2010/TSAPipelineSecurityGuidelines-12-10.pdf
APTA	Rail & Transit	Securing Control and Communications Systems in Transit Environments	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 (AVL), 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 July, 2010 Free	http://www.aptastandards.com/LinkClick.aspx?fileticket=MGtGhaNVcd0%3d&tabid=329&mid=1670&language=en-US

Appendix C – Strategic Costs By Mode

This section provides an overview of tasks, deliverables, and estimated costs between 2013 and 2017, broken down by mode. (Labor rates are based on a GS 13-10 classification.)

Highway

Year	2013	2014	2015	2016	2017
Tasks	Engage NHTSA, SAE, AASHTO, and FHWA to form a highway ICS cybersecurity standards working group	Identify and classify highway and automotive ICS systems	Write highway ICS cybersecurity standard draft	Review highway ICS cybersecurity standard	Publish highway ICS cybersecurity standard final draft
Deliverables	Meeting attendance, agendas, and minutes	Highway ICS Classification document	Draft Highway ICS Cybersecurity Standard	Revision history of Highway ICS Cybersecurity Standard	Final Draft Highway ICS Cybersecurity Standard
Cost	$115,000	$120,000	$160,000	$165,000	$170,000
Notes	Based on estimated 200 hours per year per group	Based on estimated 200 hours per year per group	Based on estimated 350 hours per year per group	Based on estimated 350 hours per year per group	Based on estimated 350 hours per year per group

Maritime

Year	2013	2014	2015	2016	2017
Tasks	Engage MARAD, USCG-CC, & ABS to form a Vessel ICS cybersecurity standards working group	Identify and classify Vessel ICS systems	Write Vessel ICS cybersecurity standard draft Engage AAPA and regional port authorities to form Port ICS cybersecurity working group	Review Vessel ICS cybersecurity standard Identify and classify Port ICS systems	Publish Vessel ICS cybersecurity standard draft
Deliverables	Meeting attendance,	Vessel ICS Classification	Draft Vessel ICS	Revision history of	Final Draft Vessel ICS

	agendas, and minutes	document	Cybersecurity Standard	Vessel ICS Cybersecurity Standard Port ICS Classification document	Cybersecurity Standard Draft Port ICS Cybersecurity Standard
Cost	$80,000	$83,000	$160,000	$165,000	$170,000
Notes	Based on estimated 200 hours per year per group	Based on estimated 200 hours per year per group	Based on estimated 400 hours per year per group	Based on estimated 400 hours per year per group	Based on estimated 400 hours per year per group

Aviation

Year	2013	2014	2015	2016	2017
Tasks	Engage ACI-NA BIT group and airports around the country to form airport ICS working group	Identify and classify Airport ICS systems Brief working group on findings	Research Aviation SDOs Write Airport ICS cybersecurity standard draft	Review Airport ICS cybersecurity standard	Publish Airport ICS cybersecurity standard final draft
Deliverables	Meeting attendance, agendas, and minutes	Airport ICS Classification document ACI-NA BIT group findings	SDO Decision Justification Draft Airport ICS Cybersecurity Standard	Revision history of Airport ICS Cybersecurity Standard	Final Draft Airport ICS Cybersecurity Standard
Cost	$60,000	$62,000	$80,000	$83,000	$86,000
Notes	Based on 200 hour estimated involvement with each group per year	Based on 200 hour estimated involvement with each group per year	Based on 350 hour estimated involvement with each group per year	Based on 350 hour estimated involvement with each group per year	Based on 350 hour estimated involvement with each group per year

Surface Transportation

Year	2013	2014	2015	2016	2017
Tasks	Review APTA standard Engage Class I operators to form Class I Rail ICS working group	Remain involved with APTA standard working group Compile cyber evaluation metrics for Class I operators	Write APTA ICS cybersecurity standard draft for buses and trucks Write freight rail ICS cybersecurity standard draft	Review APTA ICS cybersecurity standard for buses and trucks Review Freight Rail ICS cybersecurity standard	Publish Buses and Trucks ICS cybersecurity standard Publish Freight Rail ICS cybersecurity standard
Deliverables	APTA revisions Meeting attendance, agendas, and minutes	APTA working group minutes cyber evaluation metrics	Draft Buses and Trucks ICS cybersecurity Standard Draft Freight Rail ICS cybersecurity Standard	Revision history of Buses and Trucks ICS cybersecurity standard Revision history of Freight Rail ICS cybersecurity standard	Final Draft Buses and Trucks ICS cybersecurity Standard Final Draft Freight Rail ICS cybersecurity Standard
Cost	$67,000	$69,000	$80,000	$83,000	$86,000
Notes	Based on 200 hour estimated involvement with Class I railroads and 350 hour estimated involvement with APTA	Based on 200 hour estimated involvement with Class I railroads and 350 hour estimated involvement with APTA	Based on 350 hour estimated involvement with each group per year	Based on 350 hour estimated involvement with each group per year	Based on 350 hour estimated involvement with each group per year