ICS Security in Maritime Transportation

A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure

July 2013

DOT-VNTSC-MARAD-13-01

Prepared for:
Office of Security
Maritime Administration
U.S. Department of Transportation
Washington, D.C.

U.S. Department of Transportation
Research and Innovative Technology Administration
John A. Volpe National Transportation Systems Center

Volpe

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

The United States Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE July 29, 2013	3. REPORT TYPE AND DATES COVERED White Paper – June 2013

4. TITLE AND SUBTITLE

ICS Security in Maritime Transportation
A White Paper Examining the Security and Resiliency of Critical Transportation Infrastructure

5a. FUNDING NUMBERS

MA31A100 – LME07

6. AUTHOR(S)

Eric York Wallischeck

5b. CONTRACT NUMBER

None

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Department of Transportation
John A Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142-1093

8. PERFORMING ORGANIZATION REPORT NUMBER

DOT-VNTSC-MARAD-13-01

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Security
Maritime Administration
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

DOT/MARAD/MAR-420

11. SUPPLEMENTARY NOTES

None

12a. DISTRIBUTION/AVAILABILITY STATEMENT

None

12b. DISTRIBUTION CODE

None

13. ABSTRACT (Maximum 200 words)

The John A. Volpe National Transportation Systems Center was asked by the Office of Security of the Maritime Administration to examine the issue of industrial control systems (ICS) security in the Maritime Transportation System (MTS), and to develop a white paper based upon its findings for circulation amongst MTS stakeholders. In evaluating the issue, this paper first discusses the role of the MTS as part of the domestic and international transportation system and global supply chain, and provides examples of the economic impact of past natural and manmade disruptions to the MTS. It next explores the uses and applications of ICS throughout the MTS, identifies potential cybersecurity vulnerabilities of ICS, and provides examples of possible ICS failures and the potential impact on the MTS. Finally, the paper explores the issue in the context of Federal policy governing critical infrastructure, cybersecurity and supply chain resilience, and makes a number of recommendations that government agencies and the private sector might consider in order to mitigate the ICS security risks.

14. SUBJECT TERMS

Control System Security, Critical Infrastructure, DOT, Environment, Homeland Security, ICS, Industrial Control System, Industrial Control Systems, MARAD, Marine Transportation, Maritime Administration, Maritime Transportation, Preparedness, Resiliency, Resilient, Safety, Security, Transportation, Transportation Infrastructure

15. NUMBER OF PAGES

48 (inclusive)

16. PRICE CODE

N/A

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT Unlimited

SI* (MODERN METRIC) CONVERSION FACTORS

APPROXIMATE CONVERSIONS TO SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
LENGTH				
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
AREA				
in^2	square inches	645.2	square millimeters	mm^2
ft^2	square feet	0.093	square meters	m^2
yd^2	square yard	0.836	square meters	m^2
ac	acres	0.405	hectares	ha
mi^2	square miles	2.59	square kilometers	km^2
VOLUME				
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft^3	cubic feet	0.028	cubic meters	m^3
yd^3	cubic yards	0.765	cubic meters	m^3
NOTE: volumes greater than 1000 L shall be shown in m^3				
MASS				
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2000 lb)	0.907	megagrams (or "metric ton")	Mg (or "t")
oz	ounces	28.35	grams	g
TEMPERATURE (exact degrees)				
°F	Fahrenheit	5 (F-32)/9 or (F-32)/1.8	Celsius	°C
ILLUMINATION				
fc	foot-candles	10.76	lux	lx
fl	foot-Lamberts	3.426	candela/m^2	cd/m^2
FORCE and PRESSURE or STRESS				
lbf	poundforce	4.45	newtons	N
lbf/in^2	poundforce per square inch	6.89	kilopascals	kPa

APPROXIMATE CONVERSIONS FROM SI UNITS

Symbol	When You Know	Multiply By	To Find	Symbol
LENGTH				
mm	millimeters	0.039	inches	in
m	meters	3.28	feet	ft
m	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi
AREA				
mm^2	square millimeters	0.0016	square inches	in^2
m^2	square meters	10.764	square feet	ft^2
m^2	square meters	1.195	square yards	yd^2
ha	hectares	2.47	acres	ac
km^2	square kilometers	0.386	square miles	mi^2
VOLUME				
mL	milliliters	0.034	fluid ounces	fl oz
L	liters	0.264	gallons	gal
m^3	cubic meters	35.314	cubic feet	ft^3
m^3	cubic meters	1.307	cubic yards	yd^3
mL	milliliters	0.034	fluid ounces	fl oz
MASS				
g	grams	0.035	ounces	oz
kg	kilograms	2.202	pounds	lb
Mg (or "t")	megagrams (or "metric ton")	1.103	short tons (2000 lb)	T
g	grams	0.035	ounces	oz
TEMPERATURE (exact degrees)				
°C	Celsius	1.8C+32	Fahrenheit	°F
ILLUMINATION				
lx	lux	0.0929	foot-candles	fc
cd/m^2	candela/m^2	0.2919	foot-Lamberts	fl
FORCE and PRESSURE or STRESS				
N	newtons	0.225	poundforce	lbf
kPa	Kilopascals	0.145	poundforce per square inch	lbf/in^2

*SI is the symbol for the International System of Units. Appropriate rounding should be made to comply with Section 4 of ASTM E380. (Revised March 2003)

Acknowledgments

The author wishes to thank the staff of the Center for Transportation Logistics and Security at the John A. Volpe National Transportation Systems Center for their assistance in preparing this report. In particular, Director Michael G. Dinning, and members of the Security and Emergency Management Division (Division Chief John Wojtowicz, technical experts Bahar Barami, Dawn Johnson, Charles McCarthy, and David Sawin, and administrative assistant Lauren Gentile) provided valuable technical input and editorial feedback. Susan Dresley, Volpe Center Librarian, and her assistant Arthur Liu responded to numerous requests for reports and documents. At the Maritime Administration, thanks are owed to Joel Szabat, Executive Director, and Owen Doherty, Director of the Office of Security, for their interest in supporting research to address cybersecurity risks and other areas of concern to the maritime transportation system.

Contents

List of Figures

List of Tables

Photo Credits

The images in this report are from the following sources:

PAGE	SOURCE
3	Clockwise from top left: www.boeing.com/Features/2010/11/img/bca_cargo_700.jpg www.yachtdeliverycapt.com/images/towboat.jpg www.altergroup.com/blog/wp-content/uploads/2009/08/huge-container-ship.jpg http://blog.garlock.com/wp-content/uploads/2012/07/RedTractorTrailer.jpg www.montway.com/transportation/wp-content/uploads/Auto-Transport-Terminals-1024x627.jpg www.epa.gov/region1/eco/diesel/images/ports2.jpg http://bradyuselman.com/wp-content/uploads/2011/10/locomotive.jpg www.portseattle100.org/images/properties/t86/P-86_11-89.jpg
4	Top to Bottom: http://preview.turbosquid.com/Preview/2011/04/16__05_03_51/cntnr_02_01.jpgad5060bb-8a09-494f-aa44-6d9b74e76971Large.jpg http://rlv.zcache.com/diesel_passenger_train_freight_locomotive_sticker-p217402439297452668en8ct_400.jpg http://bestclipartblog.com/clipart-pics/truck-clipart-5.jpg
5	Top to Bottom: www.uacrussia.ru/common/img/uploaded/il_112/il_112_composition_1.png http://us.cdn2.123rf.com/168nwm/scanrail/scanrail1008/scanrail100800077/7701624-red-and-blue-pipelines.jpg
9	http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
10	www.interschalt.de/grafiken/3Dship_n_gr.gif
11	Drawing by the author
19	Notional drawing by the author
26	www.gao.gov/assets/650/649705.pdf

List of Abbreviations

Abbreviation	Term
AAPA	American Association of Port Authorities
ABS	American Bureau of Shipping
AMSC	Area Maritime Security Committee
CIKR	Critical Infrastructure and Key Resources
CIPAC	Critical Infrastructure Partnership Advisory Council
CLIA	Cruise Line International Association
COTS	Commercial Off The Shelf
CPU	Central Processing Unit
CSA	Chamber of Shipping of America
DHS	Department of Homeland Security
DoD	Department of Defense
DOT	Department of Transportation
FEMA	Federal Emergency Management Agency
GCC	[Transportation Sector] Government Coordinating Council
GPS	Global Positioning System
HSA-2002	Homeland Security Act of 2002
ICS	Industrial Control Systems ***[see grammatical note, below]***
ICS-CERT	Industrial Control System Cyber Emergency Response Team (an element of DHS)
ICSJWG	Industrial Control Systems Joint Working Group (an element of DHS)
ISAC	Information Sharing and Analysis Centers
LNG	Liquefied Natural Gas
MARAD	Maritime Administration
MSC	Military Sealift Command
MSCC	Maritime Sector Coordinating Council
MTS	Maritime Transportation System
NCSD	National Cyber Security Division (an element of DHS)
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NTS	National Transportation System
PPD	Presidential Policy Directive
PVA	Passenger Vessel Association
RITA	Research and Innovative Technology Administration
SCC	[Transportation] Sector Coordinating Council
SLSDC	Saint Lawrence Seaway Development Corporation
SNAME	Society of Naval Architects and Marine Engineers
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
USACE	U.S. Army Corps of Engineers
USCG	United States Coast Guard
WSC	World Shipping Council

Grammatical note: This document follows the practice of NIST Special Publication 800-82/Rev1, in which the acronym "ICS" is considered a 'plural' term, i.e. industrial control **systems*****, rather than the singular industrial control*** **system.**

Executive Summary

The John A. Volpe National Transportation Systems Center (Volpe Center) was asked by the Office of Security of the Maritime Administration (MARAD) to examine the issue of industrial control system (ICS) security in the Maritime Transportation System (MTS), and to develop a white paper for circulation amongst MTS stakeholders.

When considering potential ICS security risks in the maritime domain, one must also examine the role and scope of the MTS as part of the U.S. and international transportation system and supply chain. At its core, the MTS is critical to national security and economic stability. The MTS moves the majority of freight arriving and departing from the U.S., and carries the bulk of critical military cargoes around the globe. Consequently, any disruptions of the MTS can put national security at risk, and affect local, regional, national and even global economies. This fact has been borne out by previous maritime disruptions, both natural and manmade.

The report found that ICS vulnerabilities represent a potential risk to the security and resilience of the MTS. This conclusion is based upon four principal facts:

- ICS are ubiquitous devices found throughout the entire global transportation system. They are aboard virtually ship and in the shore-side infrastructure supporting them.
- ICS have known security vulnerabilities. These vulnerabilities can be exploited by a wide variety of hostile agents, using readily available technologies and techniques.
- ICS failures can take numerous forms. They can disable vessels, closing navigational channels or incapacitating cargo terminals. Vessel accidents caused by ICS failures can threaten passengers and crew, and significantly damage the environment. Ashore, a compromised ICS can hinder or disable cargo handling equipment, threatening safety of personnel and communities.
- Compromising an element of the MTS – whether a vessel, navigational system, port infrastructure, or another component – can disrupt the MTS and the global supply chain.

The current Federal policy framework directs U.S. Government agencies to take steps to address ICS vulnerabilities, and assigns new responsibility to DOT to ensure the security and resiliency of the nation's critical transportation infrastructure. The report's recommendations are designed to support this policy framework, as well as DOT's implicit responsibility for demonstrating federal leadership.

- Designate an agency within DOT to lead its maritime ICS security efforts; MARAD is well suited to take on this responsibility.
- Implement existing DHS and NIST recommendations concerning ICS security by leveraging the experience and technical expertise of the Volpe Center.
- Ensure that maritime cybersecurity is addressed when implementing PPD-21 and MAP-21.
- Consider establishing a maritime Critical Infrastructure Partnership Advisory Council to bring public and private stakeholders together on ICS and other maritime transportation issues.

1. Introduction

Cyber-terrorism is a significant threat to the safety, security and economy of the United States and an ever-growing concern of policy makers, emergency planners, corporate leaders and American citizens.

These concerns are well-founded. Cyber-attacks against U.S. institutions and corporations are on the rise and increasingly aimed at disabling, not just disrupting, data and systems.[1] Recent news reports of alleged nation state involvement in cyber-terrorism have sounded the alarm to the general public and increased concern about potential widespread disruptions of everyday services that rely upon computer systems. Cyber-attacks have already been directed at public transit systems, disrupting signaling and traveler information systems. Researchers have demonstrated potential vulnerabilities of a wide range of information technologies and control devices that support all modes of transportation.

The Maritime Transportation System (MTS) – like its aviation, rail, pipeline, and roadway counterparts – is subject to these same vulnerabilities and risks. Yet, the American public is generally unaware of the complexity of the MTS, and the impact that MTS disruptions pose to national security and economic stability. To most Americans, ships are floating hotels that travel to exotic ports, or the cause of disasters featured on the evening news. The public can be fixated by a cruise ship adrift at sea or a grounded oil tanker gushing oil, where their collective attention is riveted on sheen-covered seas and oil-soaked seabirds, squalid shipboard living conditions, or the search for missing seafarers. But, when considering potential threats to the global transportation system, maritime risks are often invisible.

These risks cannot be ignored since within the global transportation system, the maritime sector is the largest player. Energy and raw materials, food products and consumer goods move to and from our shores chiefly by water, with ships, tugs and barges moving more than three quarters of all global exports. A major disruption of the maritime transportation system can have a significant, immediate effect on the U.S. economy. Consider the impact of the 2002 West Coast labor dispute. Twenty-nine ports were closed, meaning supplies and goods could not reach the consumer. Anxiety and prices rose, as supplies slowed. The eleven-day shutdown cost the economy $14 billion.[2]

A broad-based cyber-attack on elements of the maritime transportation system—vessels, global navigation systems, port infrastructure, cargo management systems—can have a similar impact, as freight movement is slowed or halted. While a cyber-attack that disables a vessel transiting the Panama Canal may only affect a single waterway, it can have significant economic impact around the globe. . Cyber-attacks can also be part of criminal plots to highjack, divert or steal cargo. Attacks could be focused on stealing sensitive customer or corporate data. Resolving maritime ICS vulnerabilities is in the best interests of the safety, security and economic stability of the nation.

[1] Nicole Perlroth and David E. Sanger, "Cyberattacks Seem Meant to Destroy, Not Just Disrupt," New York Times, March 28, 2013, accessed May 1, 2013, http://nyti.ms/YHaa8D.
[2] 2002 date adjusted for inflation to reflect 2013 dollars.

2. Maritime Transportation and the Global Supply Chain

The U.S. economy relies upon the global supply chain to move its imports and exports from point of origin to final destination. Energy, raw materials and finished goods travel between continents, crisscross international land borders and move within the U.S. via a complex system of maritime, air and surface transportation and logistics networks. In 2008, that virtual "pipeline" moved $16 trillion in exports around the globe. About 13 percent of those exports – representing $2.1 trillion in materials and goods from more than 200 countries – were bound for the U.S., where they were used by 311 million Americans and 7.4 million business establishments.[3]

By any measure, marine transportation is the primary means of moving goods and raw materials to and from the U.S. In 2008, 77.7 percent of freight tonnage entering the U.S. came by water, compared to 22 percent by land and only 0.3 percent by air. When measured by value, waterborne freight represents 55 percent ($1.15 trillion) of all freight movements, compared to 25 percent ($525 billion) for freight moved by land via rail and road and 20 percent ($420 billion) transported by air.[4]

[3] U.S. Census Bureau, "Statistics of U.S. Businesses 2008," accessed May 1, 2013, http://www.census.gov/econ/susb/.
[4] U.S. Department of Transportation, Research and Innovative Technology Administration, Bureau of Transportation Statistics, *Freight Transportation: Global Highlights, 2010* (Washington, DC: 2010), accessed May 1, 2013, http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/freight_transportation/pdf/entire.pdf.

While the U.S. represents only 4.5 percent of the world's total population,[5] it accounts for twice that amount (9 percent) of worldwide container traffic, with one container out of eleven engaged in global trade either bound for or originating in the U.S.[6] In 2008, our ports handled 42.8 million containers, while 2.5 billion tons of freight was moved on our inland and coastal waterways. For comparison, 10.6 million truck containers and 2.6 million rail containers crossed by land into the U.S. from Canada and Mexico.

The maritime transportation system is part of the larger U.S. National Transportation System (NTS). The NTS ranks as the world's largest physical network in paved roadways, railways, pipelines and airports and ranks fourth (behind China, Russia and Brazil respectively) in inland and coastal waterways. Five primary modal partners operate within the NTS. In 2010, they represented the following:[7]

WATER

603 marine vessel operators, who control
40,608 commercial U.S.-flag barges, tugs and merchant ships, which operate on
25,320 miles of coastal and inland navigable waterways that serve
3,200 commercial passenger and cargo handling facilities found in
360 domestic ports[8] that handled
2,244 million metric tons of cargo including
502,212 million ton-miles of cargo moved on domestic waterways, while
5,106 **billion** ton-miles of shipboard cargo arrived at U.S. ports.[9]

RAIL

565 railroads that operate
1,332,922 locomotives and freight cars on
95,573 miles of Class I rail which moved
1,691,004 million ton-miles of freight.

ROAD

739,421 registered interstate motor carriers that operate
2,552,865 million tractor-trailer trucks on
215,633 miles of principal arterial highways and
2,414,367 miles of secondary paved roads, which together moved
1,400,000 million ton-miles of freight[10]

[5] Population Reference Bureau. *2011 World Population Data Sheet*. (Washington, DC: 2012), accessed May 1, 2013, http://www.prb.org/pdf11/2011population-data-sheet_eng.pdf.

[6] U.S. Department of Transportation, Research and Innovative Technology Administration, Bureau of Transportation Statistics. *America's Container Ports: Linking Markets at Home and Abroad*. (Washington, DC: 2011), accessed May 1, 2013, http://www.bts.gov/publications/americas_container_ports/2011/pdf/entire.pdf.

[7] U.S. Department of Transportation, Research and Innovative Technology Administration, Bureau of Transportation Statistics. *National Transportation Statistics 2012*. (Washington, DC: 2012), accessed May 1, 2013, http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/nts_entire_with_q4_updates.pdf. (2010 data unless indicated.)

[8] American Association of Port Authorities website, accessed May 1, 2013, http://www.aapa-ports.org/Industry/content.cfm?ItemNumber=1032.

[9] Calculation of 13% of 2008 global trade as reported in United Nations Conference on Trade and Development *Review of Maritime Transportation 2012.* (New York: 2012), accessed May 1, 2013, http://unctad.org/en/PublicationChapters/Chapter%201.pdf.

AIR

77 commercial air carriers that operate
7,431 commercial aircraft serving
331 major airports,[11] which moved
12,540 million ton-miles of domestic air cargo

PIPELINES

2,219 pipeline operators that manage
1,722,210 miles of oil and gas pipelines, which moved
568,400 million ton-miles of oil and gas products.[12]

Due to its global reach and freight volume, the maritime sector plays a central role in the economic security and stability of our nation. Any disruption to the maritime transportation system–whether through natural disasters, accidents, failures of infrastructure, or acts of terrorism or cybercrime–can have an immediate and cascading effect throughout the entire supply chain.

[10] 2010 data not available; reflects a projection based upon data from 1990-2003.
[11] Airports with U.S. customs facilities, as report by the Federal Aviation Administration.
[12] 2010 data not available; reflects 2009 data.

3. The Impact of Maritime Transportation System Disruptions

This paper discusses the risk and potential impact of cyber-attacks against industrial control systems in the MTS. To illustrate how such attacks could impact the MTS and the broader transportation system, one must first assess the effect that previous disruptions have had to the MTS. The following are examples of a number of natural and manmade disruptions, including assessments of their respective economic and environmental impacts.

- 1989: The *Exxon Valdez* oil spill of 1989 cost an estimated $7.0 billion in direct clean up, claims, fines and settlement expenses.[13] The indirect costs associated with this seminal disaster are even more significant. Alaskan fisheries have yet to recover from the environmental impact.[14] More rigorous industry practices required under new federal laws and regulations such as the Oil Pollution Act of 1990 added significant costs to Federal, state and local governments, ports and vessel owners and operators. Human error was deemed responsible for this incident.
- 2002: The 2002 West Coast labor dispute closed 29 ports and idled hundreds of ships for 11 days, costing the U.S. economy an estimated $11 billion.[15] Unlike natural disasters or oil spills which require repair of infrastructure or clean up, no other costs were associated with this event, so all costs can be directly attributed to the port shutdown.
- 2005: Hurricane Katrina impacted several Gulf Coast ports and brought Mississippi River traffic to a halt for nearly three weeks, backing up barge traffic throughout the inland waterway system. The estimated cost of this disaster (including clean-up, rebuilding, lost revenues, and other direct and indirect costs) runs as high as $250 billion.[16]
- 2007: The collapse of the I-35W bridge closed much of the Port of Minneapolis and brought barge traffic on portions of the Mississippi River to a halt for five weeks. This incident was attributed to design inadequacies that led to structural failures. The State of Minnesota estimated the direct economic impact of the failure exceeded $60 million, in addition to the $5 million spent by the U.S. government towards recovery efforts, and the $234 million spent to construct a replacement bridge.[17,18]
- 2010: The *Deepwater Horizon* disaster continues to have a significant economic impact on the Gulf Coast region. The direct costs to BP have exceeded $37 billion as of 2013, while the indirect

[13] International Tanker Owners Pollution Federation statistics, accessed May 1, 2013, http://www.itopf.com/spill-compensation/cost-of-spills/.

[14] Exxon Valdez Oil Spill Trustee Council, accessed May 1, 2013, http://www.evostc.state.ak.us/recovery/status_herring.cfm.

[15] Tim Reid and Steve Gorman, "Cost of Union Dock Strike in CA: $1B a Day," Reuters, December 3, 2012, accessed May 1, 2013, http://www.thefiscaltimes.com/Articles/2012/12/03/Cost-of-Union-Dock-Strike-in-CA-1B-a-Day.aspx#page1.

[16] University of North Texas report, accessed May 1, 2013, https://news.unt.edu/news-releases/unt-experts-can-discuss-tropical-storm-gustav-and-hurricane-katrinas-3rd-anniversary.

[17] Department of Employment and Economic Impact, "Economic Impacts of the I-35W Bridge Collapse, September 4, 2007, accessed May 1, 2013, http://www.dot.state.mn.us/i35wbridge/rebuild/municipal-consent/economic-impact.pdf.

[18] Federal Highway Administration press release, accessed May 1, 2013, http://www.fhwa.dot.gov/pressroom/dot0774.cfm.

impact on area fisheries, the tourism industry and other businesses continues to be assessed. This incident has been attributed to equipment failure and human error.

- 2011: The Japan earthquake and tsunami closed 15 major shipping ports for two weeks, affecting cargo flow throughout the Pacific basin. The World Bank estimated the total cost of this disaster to be between $122 billion and $235 billion.[19]
- 2012: Major droughts affected water levels on the Mississippi River system, which moves 60 percent of all domestic grain shipments and 22 percent of petroleum products.[20] Lower water levels meant barges are not fully loaded and traffic was slowed due to navigational restrictions. Other cargoes were shifted to rail and road, burdening systems already operating at capacity. On the Great Lakes, lower water levels meant ships were forced to carry less cargo per voyage, thereby increasing the number of ship voyages needed to move cargoes, with associated increases in risk and air pollution.
- 2012: Hurricane Sandy affected the Port of New York and New Jersey, with ripple effects felt at other East Coast feeder ports. Cargo delays alone were estimated at nearly $1.0 billion,[21] with all direct and indirect costs anticipated to exceed $50 billion.[22]
- 2013: The grounding of the U.S.S. *Guardian* in the Philippines' Sulu Sea will cost in excess of $300M (loss of ship and salvage costs), plus losses due to environmental damage inflicted on Tubbataha Reef and potential loss of tourism. Preliminary investigation into the cause of the accident includes inaccurate navigational data on the vessel's U.S. government digital charts.
- 2013: Separate incidents involving four cruise ships (the *Carnival Triumph*, *Carnival Elation*, *Carnival Dream* and *Carnival Legend*) affected vessel propulsion and operating systems. Lives and health of passengers and crew were put at risk. Preliminary investigation into each incident identified mechanical and system failures as the likely causes.

Each of these disruptions had a variety of effects. Communities, ports and transportation infrastructure were strained as they sought to respond and recover. In some cases, components of the U.S. NTS were shut down, delaying cargos at the cost and inconvenience of buyers and sellers. In other cases, regional economies were affected and lives impacted due to the inability of the transportation system to restore freight movement and core transportation services in a timely manner. Businesses and consumers were affected, as shippers were forced to use other transportation modes – often lengthier, slower and more costly – to re-route cargo.

[19] "East Asia and Pacific Economic Update 2011, Vol. 1." Washington: World Bank, March 2011, accessed May 1, 2013, http://siteresources.worldbank.org/inteaphalfyearlyupdate/Resources/550192-1300567391916/EAP_Update_March2011_japan.pdf.

[20] Climatewire news story, July 2012, accessed May 1, 2013, http://eenews.net/public/climatewire/2012/07/27/1.

[21] USA Today, November 2, 2012, accessed May 1, 2013, http://www.usatoday.com/story/news/nation/2012/11/02/cargo-recovering/1678243/

[22] National Hurricane Center. *Tropical Cyclone Report: Hurricane Sandy.* Miami: NOAA, February 2013, accessed May 1, 2013, http://www.nhc.noaa.gov/data/tcr/AL182012_Sandy.pdf.

4. Industrial Control Systems in the Maritime Transportation System

4.1 Industrial Control System Operation

It is helpful to understand the basic operation of an industrial control system (ICS), to provide a sense of its operation, widespread application and large number of devices used in the transportation system. According to the National Institute of Standards and Technology (NIST):[23]

> *Industrial control systems include supervisory control and data acquisition (SCADA) systems, distributed control systems and programmable logic controllers.*[24] *The scope of facilities and equipment encompassed by these technologies range from broadly dispersed operations, such as natural gas pipelines and water distribution systems, down to individual machines and processes.*
>
> *Most industrial control systems 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 IT offerings have been integrated into most such systems. 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, these systems must operate continuously and reliably, often around the clock. Unlike information technology (IT) systems, which process, store and transmit digital data, industrial control systems typically monitor the system environment and control physical objects and devices, such as pipeline valves. Disruptions or failures can result in death or injury, property damage and loss of critical services.*

A typical installation includes a dedicated CPU (a computer processor chip) running a controller device. The controller monitors a data input and then makes adjustments as needed to control a process. For example, a sensor measures a speed, temperature or pressure. When the measured value diverges from programmed norms, adjustments are made through an actuator to speed up or slow down a motor, raise or lower a temperature, or open or close a valve (see Figure 1).[25]

[23] Definition from the National Institute of Standards and Technology, accessed May 1, 2013, http://www.nist.gov/el/isd/ics-062111.cfm.

[24] Other common types of systems involving industrial control devices include emergency management systems (EMS), automated systems (AS), safety instrumentation systems (SIS), and remote terminal units (RTU).

[25] Stouffer, Falco, Scarfone, "Guide to Industrial Control Systems (ICS) Security" NIST SP 800-82, Washington: NIST, 2011, accessed May 1, 2013, http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

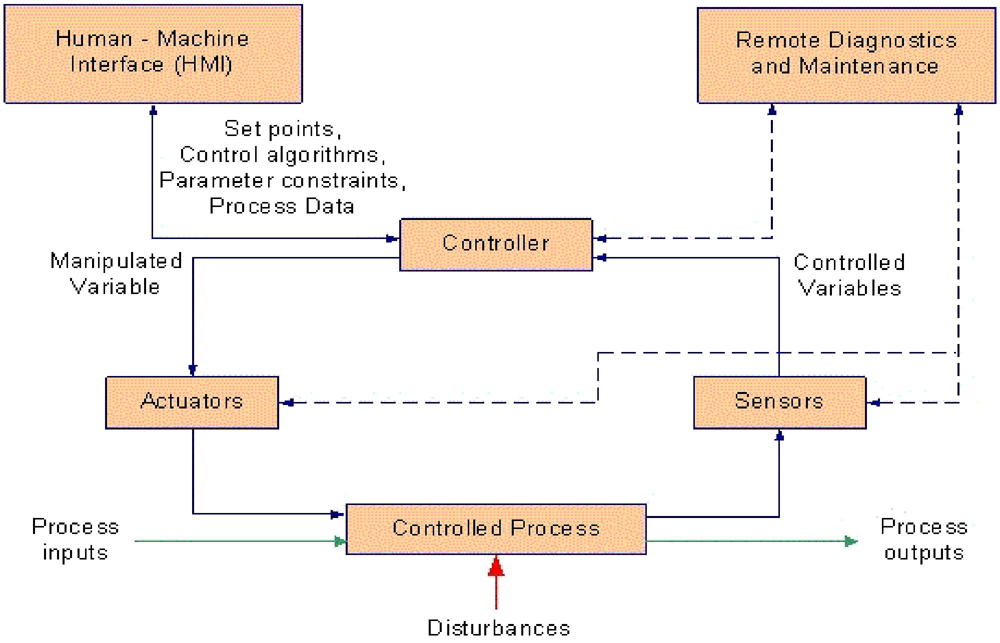

Human - Machine Interface (HMI)
Remote Diagnostics and Maintenance
Set points, Control algorithms, Parameter constraints, Process Data
Controller
Manipulated Variable
Controlled Variables
Actuators
Sensors
Process inputs
Controlled Process
Process outputs
Disturbances

Figure 1: Schematic Operation of Typical Industrial Control Systems

Despite their use of a computer chip (CPU), ICS are often viewed as a mechanical control device than a computer device. Consequently, process owners, system operators and technicians were historically viewed as responsible for management, operation and security of ICS, rather than network or IT systems managers and administrators. That is no longer the case:[26]

> *Initially, ICS had little resemblance to traditional information technology (IT) systems in that ICS were isolated systems running proprietary control protocols using specialized hardware and software. Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents. As ICS are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are starting to resemble IT systems....*
>
> *Although some characteristics are similar, ICS also have characteristics that differ from traditional information processing systems. Many of these differences stem from the fact that logic executing in ICS has a direct effect on the physical world. Some of these characteristics include significant risk to the health and safety of human lives and serious damage to the environment, as well as serious financial issues such as production losses, negative impact to a nation's economy, and compromise of proprietary information. ICS have unique performance and reliability requirements and often use operating systems and applications that may be considered unconventional to typical IT personnel. Furthermore, the goals of safety and efficiency sometimes conflict with security in the design and operation of control systems.*

[26] Stouffer, Falco, Scarfone, "Guide to Industrial Control Systems (ICS) Security" NIST SP 800-82, Revision 1, Washington: NIST, 2013, pg.1, accessed July 18, 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf.

4.2 Maritime Applications of Industrial Control Systems

In a 2012 report for the Department of Homeland Security (DHS) Industrial Control System Cyber Emergency Response Team (ICS-CERT), the John A. Volpe National Transportation Systems Center (Volpe Center) inventoried ICS found in typical marine applications. Volpe experts identified hundreds of ICS installed aboard cargo ships (Figure 2), and throughout the infrastructure that supports vessel operation and navigation, and the loading, discharge and movement of cargo at the marine-land intermodal connection (see Figure 3).

- Commercial merchant ships rely upon hundreds of ICS to manage propulsion, support navigation and communications, provide fire protection, operate safety systems, and manage cargo loading and discharge.
- ICS are also found aboard the support vessels such as pilot boats, tugboats, fireboats and oil spill response vessels, which ensure the safe movement of vessels and their cargo while entering and leaving port and which monitor their safety while berthed at passenger and cargo terminals.
- Many navigation systems, navigational aids, and vessel traffic management systems used by the U.S. Coast Guard (USCG) to safely guide vessels on the waterways have integrated ICS.
- ICS often control the mechanical systems that operate locks and dams, such as those found on the St. Lawrence Seaway, Panama Canal and throughout the Mississippi River waterway.
- ICS are found in the dock-side container cranes, straddle-carriers and autonomous vehicles that load, unload and transport containers in a modern port, and in the bulk liquid and dry cargo handling systems that load and unload grain, ore, crude oil, diesel, toxic chemicals and LNG.

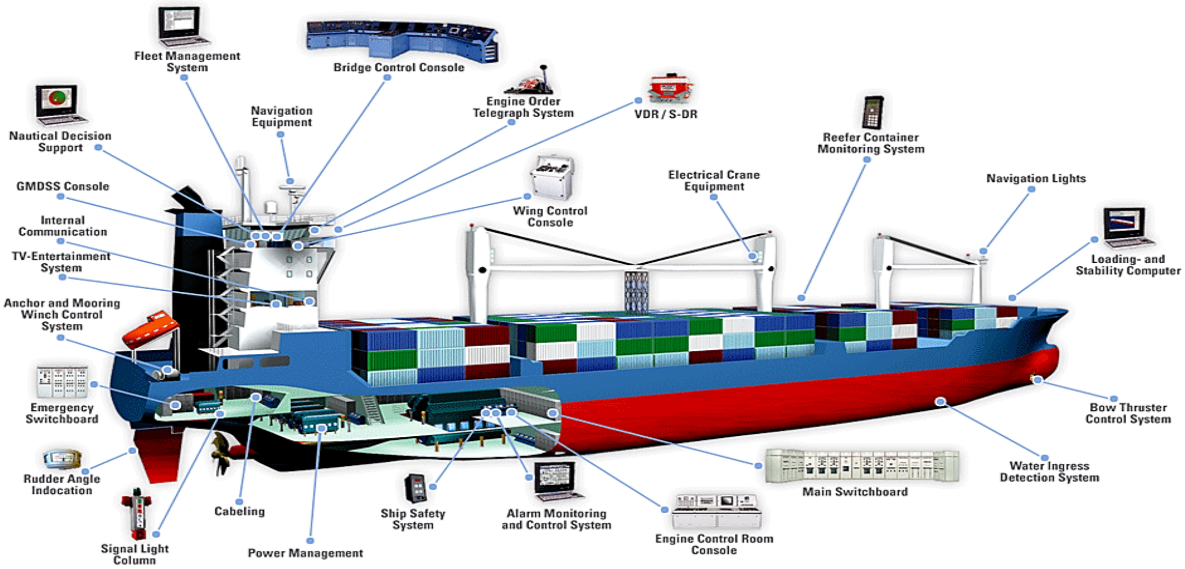

Fleet Management System
Bridge Control Console
Engine Order Telegraph System
VDR / S-DR
Navigation Equipment
Nautical Decision Support
Reefer Container Monitoring System
GMDSS Console
Electrical Crane Equipment
Navigation Lights
Wing Control Console
Internal Communication
TV-Entertainment System
Loading- and Stability Computer
Anchor and Mooring Winch Control System
Emergency Switchboard
Bow Thruster Control System
Water Ingress Detection System
Rudder Angle Indocation
Main Switchboard
Cabeling
Ship Safety System
Alarm Monitoring and Control System
Engine Control Room Console
Signal Light Column
Power Management

Figure 2: Typical Shipboard Industrial Control Systems

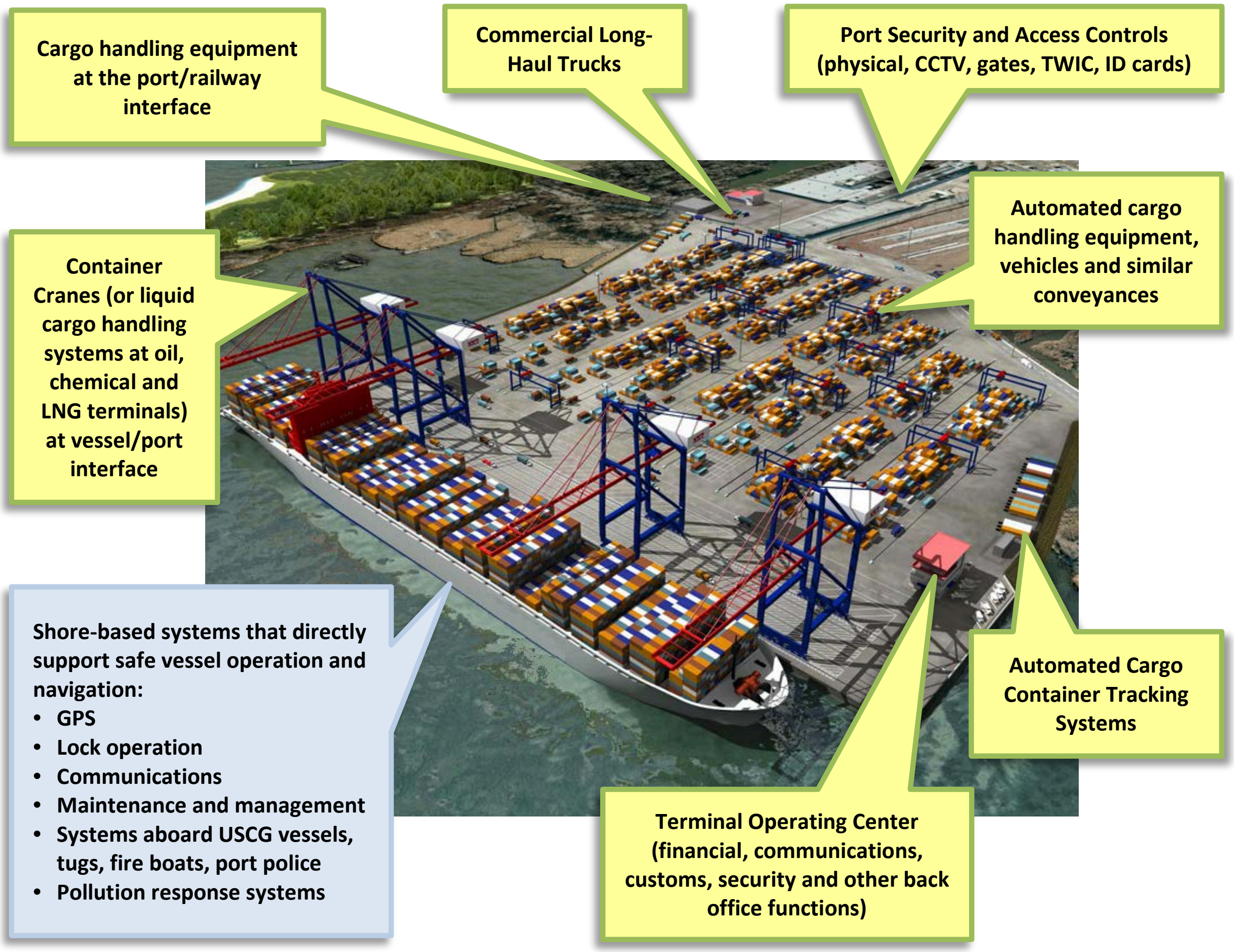

Cargo handling equipment at the port/railway interface
Commercial Long-Haul Trucks
Port Security and Access Controls (physical, CCTV, gates, TWIC, ID cards)
Automated cargo handling equipment, vehicles and similar conveyances
Container Cranes (or liquid cargo handling systems at oil, chemical and LNG terminals) at vessel/port interface
Shore-based systems that directly support safe vessel operation and navigation:
• GPS
• Lock operation
• Communications
• Maintenance and management
• Systems aboard USCG vessels, tugs, fire boats, port police
• Pollution response systems
Automated Cargo Container Tracking Systems
Terminal Operating Center (financial, communications, customs, security and other back office functions)

Figure 3: Typical Shore-based, Maritime Transportation System Industrial Control Systems

4.3 Industrial Control System Vulnerabilities

The Department of Homeland Security's National Cybersecurity Division's Transportation Sector Working Group identified several vulnerabilities of industrial control systems:[27]

- Reliance on commercial off-the-shelf (COTS) technologies. Early ICS were stand-alone systems, often with propriety technology not widely available. In contrast, newer ICS primarily use COTS technologies that are connected to other systems and technologies. These COTS systems are network-based and use common standards for communication protocols. Standard operating systems such as Windows, UNIX, or Linux are increasingly used in ICS. Use of wireless devices and trends towards Bring Your Own Devices (BYOD) for navigation, trip information and other purposes can introduce vulnerabilities if not properly configured.

[27] Department of Homeland Security, U.S. Cyber Emergency Response Team, "Roadmap to Secure Control Systems in the Transportation Sector," Washington, DC: August 2012, accessed May 1, 2013, http://www.us-cert.gov/control_systems/pdf/TransportationRoadmap083112.pdf.

- Connectivity. Modern ICS are connected to company enterprise systems that rely on common operating platforms and Internet accessibility through public-switched telephone, cable, or wireless networks. Many ICS are also Internet Protocol (IP) addressable. These features give asset owners and operators immediate benefits by extending connectivity and interoperability with other IT infrastructures.
- Interdependency. Failures within one transportation sector can spread into other modes, due to the high degree of interdependency among transportation infrastructure systems. A successful cyber-attack might be able to take advantage of these interdependencies to amplify the overall risk and produce cascading impacts across multiple systems, and significantly increase economic damage. For example, an attack on a container terminal management system could disrupt intermodal container services involving maritime, rail and truck transportation.
- Complexity. The demand for real-time information-sharing and control has increased system complexity in several ways. Access to ICS is being granted to more users; business and control systems are interconnected; and the degree of interdependency among infrastructures has increased. Disconnects between the professionals who administer IT network security and the operators and technicians responsible for control system devices have led to challenges in effectively coordinating network security between these two key groups.
- Continued use of legacy systems. Older legacy ICS often operate in more independent modes and tend to have inadequate password policies and security administration, no data protection mechanisms and protocols that are prone to snooping, interruption and interception. Insecure legacy systems have long service lives and will remain vulnerable until security issues 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 outsourcing ICS support, service and maintenance to third parties located in foreign countries.
- Information availability. Attackers no longer need to be control operations experts to access ICS. Many ICS manuals and training videos are publicly available and many hacker tools can now be downloaded from the Internet and applied with limited system knowledge.
- 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.

4.4 Types and Impacts of ICS Exploits

ICS are used to manage processes that operate mechanical devices. These devices make things or move things, or control larger machines that move people or cargo. Exploiting an ICS vulnerability can therefore have a broad range of impacts and consequences:

- Direct physical damage to affected equipment and systems. When a controlled variable such as speed, temperature or pressure is exploited, the controlled mechanism can fail with catastrophic results: a machine over-speeds, melts or catches fire, or explodes. The resulting damage can affect a single piece of equipment, interrupting a larger system, which can disable or destroy an entire ship.

- Small-scale, local disruptions. Such disturbances would be limited in scope, damaging or interrupting individual systems or single ships within a single organization, without widespread impact beyond the affected function or service. While such "nuisance disruptions" would have limited impact to the MTS, NTS or global supply chain, they begin to introduce levels of unreliability and unpredictability that may have far more widespread economic and operational consequences.

- Injury or death to operators, passengers or the general public. Depending upon the nature of a targeted ICS and the extent of damage caused by its failure, an incident can affect an individual machinery operator or a larger group of workers or bystanders. Under certain conditions, damage to a large vessel or other conveyance can injure dozens of crew or passengers. A cataclysmic explosion due to failure of a critical safety system can maim or kill hundreds of civilians.

- Catastrophic disruptions to the transportation system. A sunken vessel blocking a shipping channel, a major explosion at an oil or LNG discharge facility, sabotage to canal locks, or a series of mishaps involving cargo container cranes in critical ports can have long-term impacts to the safety, stability and reliability of elements of the transportation system.

Unlike other disruptions, cyber-attacks against ICS can initially appear to have been caused by a mechanical failure or human error. It often takes investigators weeks or months to connect the failure to the exploit of a cybersecurity vulnerability. Malware could also be designed to be dormant until certain parameters are met, such as vessel speed or location, or a specific date and time. In this way, a series of seemingly unrelated equipment failures around the world might actually represent a coordinated attack on identical systems used by different global operators.

Vulnerabilities in ICS can be exploited in numerous ways, with varying impacts. Yet, the threat those vulnerabilities pose usually receives little public attention. It wasn't until 2010, when the Stuxnet computer virus was used to disable industrial centrifuges used in the production of weapons-grade nuclear material, that the general public learned of the potential use of a new kind of cyber "weapon".[28]

[28] David Kushner, "The Real Story of Stuxnet," IEEE Spectrum, March 2013, accessed May 1, 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

The 2010 Stuxnet attack was a watershed event, and changed the way that government officials, industry leaders, and private citizens looked at cyber-attacks. The Stuxnet attack was widely viewed as a beneficial, defensible use of cyber-weapons technology, since the intent of the cyber-attack was to disrupt and disable a potential terror state's nuclear weapons capability. However, it is important to recognize that the same techniques used in that incident could be used to disable comparable systems used worldwide in systems that manage other infrastructure systems, including the safe and reliable movement of cargo and passengers.

Stuxnet also revealed that cybersecurity incidents were no longer simply limited to thefts of identify, banking information, or sensitive national security information. Now, hostile agents -- employees or other insiders, and terrorists at home and abroad – had a powerful, invisible weapon at their disposal.

In the three years since Stuxnet surfaced, the threat has grown. A respected cybersecurity firm reported in 2013 that cyber-espionage units operating in Communist China successfully compromised the networks of over 141 U.S. companies, stealing vast quantities and wide varieties of intellectual property.[29] Among the targets were private companies that control the natural gas system, water supply and power grid.[30] By accessing the networks of critical utility networks, an attacker can introduce a cyber-weapon that exploits the ICS used to safely control and manage those utility systems.

The Stuxnet attack was not the first time that computer-based technology was used to exploit a cybersecurity vulnerability. Each of the following examples describes other failures of computer-based components or controllers, which led to the malfunction of critical safety or operating systems.

- In 2003, the Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant, disabling a safety monitoring system for over 5 hours before the failure was noticed.[31]
- In 2003, a computer bug, buried deep within millions of lines of computer code for a GE power plant management system, causes an alarm system to fail at an Ohio power plant, initiating a cascading black out that darkened 50 million homes across eight states and Canada.[32]
- In 2009, a crowded Metro train in Washington, DC, collided with another train stopped on the same tracks, killing nine people and sending 52 others to the hospital. The NTSB determined that the automatic train control system used to manage system traffic lost detection of the stalled train and continued to transmit speed commands to the moving train until point of impact.[33] Automatic train control system are remotely controlled and accessed.

[29] "APT1: Exposing One of China's Cyber Espionage Units." Washington: Mandiant, 2012, accessed May 1, 2013, http://intelreport.mandiant.com/.

[30] Cybersecurity vulnerabilities in the nation's electric power delivery system have been previously identified by the National Research Council in a declassified 2007 report: National Research Council. Terrorism and the Electric Power Delivery System. Washington, DC: The National Academies Press, 2012, accessed May 1, 2013, http://www.nap.edu/catalog.php?record_id=12050.

[31] SecurityFocus news article, August 2003, accessed May 1, 2013, http://www.securityfocus.com/news/6767.

[32] SecurityFocus new story, February 2004, accessed May 1, 2013, http://www.securityfocus.com/news/8016.

[33] "Collision of Two Washington Metropolitan Area Transit Authority Metrorail Trains Near Fort Totten Station, Washington, DC, June 22, 2009". Washington: National Transportation Safety Board, 2010, accessed May 1, 2013,

Researchers have demonstrated numerous methods to hack into the dozens of computer chips found on modern automobiles, trucks, tractors, industrial vehicles, and vessels, to successfully disable critical systems and safety features.[34] In the fall of 2012, the FBI issued a cyber-alert bulletin that described the unauthorized access of a building's automated and remotely managed HVAC systems. The compromised control system is used for over 300,000 other applications worldwide, including energy management, building automation, telecommunications, security automation and lighting control.[35]

Researchers have also warned of the vulnerability of Global Positioning System (GPS) receivers. These systems are vulnerable to a number of different attacks such as blocking and jamming (which prevents locking onto a position), or spoofing (which feeds the receiver false information so that it computes an erroneous time or location).[36] Interfering with a GPS signal can impact systems far beyond those used for navigation, since many everyday processes rely upon GPS time signals for operation.

http://www.ntsb.gov/doclib/reports/2010/RAR1002.pdf.

[34] Aliya Sternstein, "Is Carhacking a Serious Threat? Some Analysts Think So.", Nextgov, March 8, 2013, accessed May 1, 2013, http://www.nextgov.com/emerging-tech/2013/03/carhacking/61774/?oref=govexec_today_nl.

[35] "Situational Information Report 00000003417, 23 July 2012." Washington: Federal Bureau of Investigation. http://info.publicintelligence.net/FBI-AntisecICS.pdf.

[36] Nighswander, et. al. "GPS Software Attacks." Pittsburgh: Carnegie-Mellon University, 2012, accessed May 1, 2013, http://users.ece.cmu.edu/~dbrumley/courses/18487-f12/readings/Nov28_GPS.pdf.

5. Federal Policy Framework

5.1 National Preparedness

National Preparedness has its roots in federal disaster planning and response. As early as 1803, the Federal government recognized it had a responsibility to its citizens during times of hardship, when it passed legislation providing relief from customs duties for “sufferers by fire, in the town of Portsmouth [New Hampshire]”.[37] Over the ensuing decades, the federal government responded on an ad hoc basis to hurricanes, floods, fires, tornadoes, and earthquakes with over 100 individual pieces of legislation.

Several laws were passed that addressed facets of preparedness and emergency response, such as the Flood Control Act of 1936, which recognized the need to protect citizens from “menace[s] to national welfare”. Later, the National Flood Insurance Act of 1968 offered new flood protection to homeowners and the Disaster Relief Act of 1974 established the process of Presidential disaster declarations. Numerous federal agencies were involved in disaster response, creating confusion and lack of coordination. In 1979, Executive Order 12127 was signed to create the Federal Emergency Management Agency (FEMA) to centralize responsibility for federal disaster planning and response.[38]

Following the terrorist attacks of September 11, 2001, the focus of preparedness policy was expanded to include terrorism. The government now uses an all-hazards approach to planning, preparation, response, and recovery, often building upon the civil defense experience of World War 2 and the Cold War (e.g., vigilance against saboteurs, emergency stockpiles at home). The Homeland Security Act of 2002 assigned responsibility for coordinating emergency preparedness efforts to the Department of Homeland Security.[39] More recently, Presidential Policy Directive (PPD) 8, “National Preparedness” (December 2011) set forth more detailed goals and objectives for federal preparedness policy.[40]

5.2 Infrastructure Security and Resilience

The Homeland Security Act of 2002 (Public Law 107-296)[41] outlines the framework of responsibility for protecting the nation’s Critical Infrastructure and Key Resources (CIKR). One of its requirements is the development of a National Infrastructure Protection Plan (NIPP)[42] that addresses the security and

[37] A Century of Lawmaking for a New Nation: U.S. Congressional Documents and Debates, 1774 - 1875 Statutes at Large, 7th Congress, 2nd Session, Chap. 6, accessed May 1, 2013, http://memory.loc.gov/cgi-bin/ampage?collId=llsl&fileName=002/llsl002.db&recNum=238.

[38] Federal Emergency Management Agency website, accessed May 1, 2013, http://www.fema.gov/about-agency.

[39] Public Law 107-296, “Homeland Security Act of 2002,” accessed May 1, 2013, http://www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf.

[40] Presidential Policy Directive 8 (PPD-8), “National Preparedness” March 30, 2011, accessed May 1, 2013, www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf.

[41] Op. cit.

[42] Department of Homeland Security, “National Infrastructure Protection Plan, 2009,” accessed May 1, 2013, www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

resiliency of each infrastructure sector. The NIPP is managed and implemented by DHS. Last updated in 2009, the NIPP represents the collaboration between federal, state and local level agencies and their private sector partners.

The stated objective of the NIPP is to build a *safer*, more *secure* and more *resilient* America by preventing, deterring, neutralizing and mitigating the effects of a terrorist attack or natural disaster and to strengthen national preparedness, response and recovery in the event of an emergency. In support of the NIPP, infrastructure protection plans were developed for each CIKR sector. These Sector-Specific Plans (SSPs) provide a unifying framework that integrates federal, state, local and private sector efforts.

In February 2013, the White House issued PPD-21, "Critical Infrastructure Security and Resilience" (February 2013).[43] It recognizes that the approaches used to prepare, plan and mitigate the impact of a terrorist attack can be applied in an *all-hazards* environment. Taking an all-hazards approach merges the comprehensive body of work to prepare for, respond to and recover from natural disasters with the more specialized research and planning associated with security threats and acts of terrorism. PPD-21 also recognizes that infrastructure systems must be inherently *secure* when initially designed and placed into service, yet *resilient* because disruptions of one form or another are inevitable.

Addressing resilience in transportation planning mitigates the risks in an all-hazards environment, in terms of loss of life or property, and natural and economic resources. Examples of hazard planning include structural preparations for natural disasters such as hurricanes, but also include comprehensive systems analysis, contingency planning, education and outreach. Agencies and industries that actively engage in assessing and mitigating against risks and address resiliency as part of that process, are less susceptible to disruptions, are able to recover faster from disruptions that do occur and experience lower economic impacts than those entities which do not engage in these activities.

5.3 Cybersecurity

ICS are essentially computer-based systems and fall under the jurisdiction of many of the laws and regulations that govern cybersecurity.[44] The White House has also addressed cybersecurity issues at a policy level through the following:

- "Comprehensive National Cybersecurity Initiative"[45]
- National Security Presidential Directive 54 / Homeland Security Presidential Directive 23 "Cyber Security and Monitoring" (2008)[46]

[43] Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience" February 12, 2013, accessed May 1, 2013, www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[44] For example, see Eric A. Fisher, "Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions." Washington: Congressional Research Service, November 9, 2012, accessed May 1, 2013, www.fas.org/sgp/crs/natsec/R42114.pdf.

[45] "The Comprehensive National Cybersecurity Initiative." Washington: White House, 2010, accessed May 1, 2013, (www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

[46] NSPD 54 is a classified document and references are not publicly available.

- Cyberspace Policy Review 2009, "Assuring a Trusted and Resilient Information and Communications Infrastructure"[47]
- Presidential Policy Directive 21, "Critical Infrastructure Security and Resilience" (2013)
- Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (2013)[48]

In 2009, DHS issued a "Strategy for Securing Control Systems: Coordinating and Guiding Federal, State and Private Sector Initiatives," which provides broad policy and program guidelines for addressing the issue across all infrastructure environments.[49] This strategy was augmented with a more detailed set of recommendations for the transportation sector, the "Roadmap to Secure Control Systems in the Transportation Sector" (2012).

5.4 Global Supply Chain Security and Resilience

The vulnerabilities associated with industrial control systems represent a clear and significant risk to supply chain resiliency and efficiency. The "National Strategy for Global Supply Chain Security" issued in January 2012 adopts a comprehensive, all-hazards approach that focuses on security, efficiency and resilience.[50] The Strategy identified two overarching goals:

- *Efficiency and security*, to promote the timely, efficient flow of legitimate commerce while protecting and securing the supply chain from exploitation and reducing its vulnerability to disruption.
- *Resilience*, whereby the supply chain is prepared for and can withstand, evolving threats and hazards and can recover rapidly from disruptions.

A 2012 Report by the World Economic Forum, "New Models for Addressing Supply Chain and Transport Risk",[51] advocates the all hazards approach to supply chain security [emphasis added]:

> *Systemic risks within supply chain and transport networks are characterized by an unexpected trigger event and a network setup that cannot absorb the shock and knock-on effects. The initial event results in a cascading disruption or failure across regions or industries.*
>
> *However, prediction of specific disruptions is felt to be less important than having the resiliency in place for effective response,* ***no matter what the cause****. While highlighting industry robustness in the face of recent shocks, experts identified the vulnerabilities of most concern that limit the resilience of supply chain and transport networks.*

[47] "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure" Washington: White House, 2009, accessed May 1, 2013, www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[48] Presidential Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" February 12, 2013, accessed May 1, 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[49] "Strategy for Securing Control Systems: Coordinating and Guiding Federal, State and Private Sector Initiatives." Washington: Department of Homeland Security, October 2009, accessed May 1, 2013, (https://ics-cert.us-cert.gov/pdf/Strategy%20for%20Securing%20Control%20Systems.pdf)

[50] "National Strategy for Global Supply Chain Security." Washington: White House, January 2012, accessed May 1, 2013, (http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf)

[51] "New Models for Addressing Supply Chain and Transport Risk". Geneva: World Economic Forum, 2012, p.4, accessed May 1, 2013, www3.weforum.org/docs/WEF_SCT_RRN_NewModelsAddressingSupplyChainTransportRisk_IndustryAgenda_2012.pdf.

5.5 Federal Policy Framework

The four areas outlined above represent the Federal policy framework. Within that framework, control system security becomes central to both *Critical Infrastructure Security and Resilience* and *Global Supply Chain Security*, as illustrated in Figure 4.

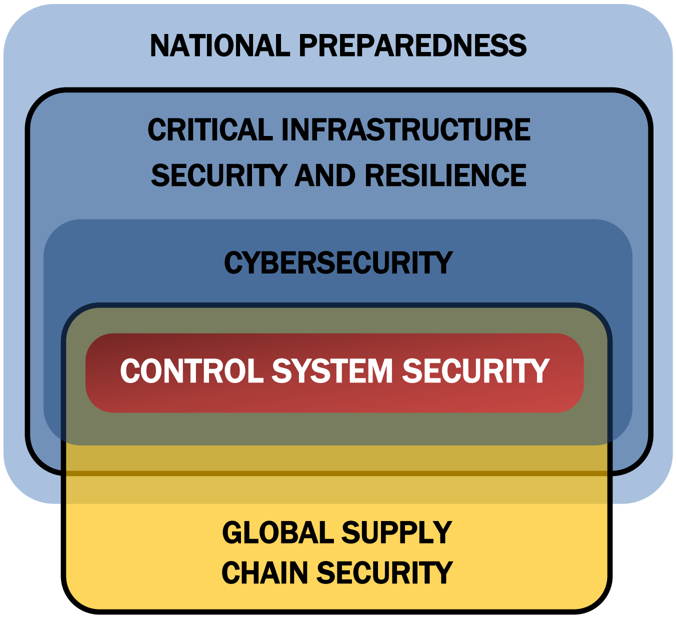

NATIONAL PREPAREDNESS
CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE
CYBERSECURITY
CONTROL SYSTEM SECURITY
GLOBAL SUPPLY CHAIN SECURITY

Figure 4: Notional Overlap of Federal Policy Concerning Control System Security

The concept of *resilience* has gained standing with government and private sector officials since it represents an effective marriage of system design, owner planning and preparation, operator response and overall system recovery. It allows for system owners to apply risk-based strategies suitable to specific systems and functions, making it adaptable and cost effective.

In this context, resilience focuses on four key components of system and component design and operation:

- ***Fault-tolerance (prevention);***
- ***Adaptation (situational awareness and smart real-time problem solving);***
- ***Redundancy (capability for asset substitution and avoidance of single-point failure);***
- ***Post-event response/recovery and mitigation.***

Resilient design, planning and operation have become fundamental best practices for public and private stakeholders.

6. Maritime Control System Stakeholders

6.1 Federal Agency Partners

Beyond the White House and the Executive Office of the President, three Cabinet departments and their related agencies have interests in addressing maritime industrial control system vulnerabilities.

6.1.1 DEPARTMENT OF TRANSPORTATION

PPD-21 assigned the Department of Transportation (DOT) as a co-Sector Specific Agency (SSA), along with DHS, with responsibility for transportation systems within the NIPP. Previously, DHS had sole responsibility for the transportation sector, with responsibility for maritime transportation delegated to the U.S. Coast Guard. This change is significant for a number of reasons:

- The complementary resources of two cabinet departments are brought to bear.
- DOT is responsible for evaluating issues across all modes of transportation, and recognizes the interdependencies of, and overlaps between, each modal transportation systems.
- DOT has experience in harmonizing federal transportation goals with those of states, regions and the private sector.

6.1.1.1 Office of the Secretary of Transportation

There are three elements within the Office of the Secretary of Transportation (OST) which are involved with ICS security issues:

- The Office of Transportation Policy (OST-P), under the leadership of the Under Secretary for Policy, recommends overall transportation policy initiatives to the Secretary, and coordinates multi-modal initiatives and processes. OST-P is responsible for developing a Transportation Resiliency Policy.
- The Office of Intelligence, Security and Emergency Response (S-60) is responsible for developing, coordinating and executing plans and procedures which balance transportation security requirements with safety, mobility and economic needs. With the implementation of PPD-21, it can be expected that S-60 will take on a significant role in coordinating policy across all transportation modes.
- The DOT Safety Council Cyber Security Action Team was established to ensure that cybersecurity issues are addressed, particularly in safety-critical transportation systems.

6.1.1.2 Maritime Administration

The Maritime Administration (MARAD) is the DOT agency responsible for the maritime transportation sector. MARAD's programs promote the use of waterborne transportation and its seamless integration with other segments of the transportation system. MARAD also promotes the viability of the U.S. merchant marine as a cost-effective transportation solution. MARAD works in other policy and program areas involving ships and shipping, shipbuilding, port operations, vessel operations, national security, environment and safety. MARAD also maintains a fleet of cargo ships in reserve, which provide surge sealift during war and national emergencies.

6.1.1.3 Saint Lawrence Seaway Development Corporation

The Saint Lawrence Seaway Development Corporation (SLSDC) and its Canadian counterpart, the St. Lawrence Seaway Management Corporation (SLSMC), are responsible for the operation and maintenance of the Saint Lawrence Seaway (the Seaway), a 2,340 mile, deep-draft waterway extending from the Atlantic Ocean to the head of the Great Lakes. The SLSDC is a wholly owned government corporation, while the SLSMC is a not-for-profit corporation.

The SLSDC has shown considerable leadership in addressing safety, security and environmental issues faced by the Seaway, which could impact its surrounding communities and watershed and the companies operating vessels along its route. Consequently, the SLSDC can play an effective role in facilitating discussion of ICS vulnerabilities, risks and mitigation efforts.

6.1.1.4 John A. Volpe National Transportation Systems Center

As DOT's multimodal research entity, the John A. Volpe National Transportation Systems Center (Volpe Center), a part of the Research and Innovative Technology Administration, has amassed considerable research experience in assessing the vulnerabilities and risks associated with industrial control systems, as well as many other transportation issues. Its experts are working closely with technical experts throughout the federal government to develop mitigation strategies and solutions for cybersecurity vulnerabilities in transportation. Perhaps most important, the Volpe Center has experience in developing technical solutions across all transportation modes, which allows it to develop system-wide recommendations and strategies, which can avoid stove-pipe solutions focused on single modes of transportation.

6.1.2 DEPARTMENT OF HOMELAND SECURITY

DHS is the leading federal entity with responsibility for overall national preparedness, security and infrastructure protection. PPD-21 designates DHS as a co-Sector Specific Agency responsible (along with DOT) for transportation systems within the NIPP. Within DHS, there are several organizational components with responsibility for ICS security maritime transportation issues:

6.1.2.1 Science and Technology Directorate, Cybersecurity Division

The Cybersecurity Division (CSD) was established in 2011, to "…contribute to enhancing the security and resilience of the Nation's critical information infrastructure and the Internet by (1) driving security improvements to address critical weaknesses, (2) discovering new solutions for emerging cyber security threats and (3) delivering new, tested technologies to defend against cyber security threats."[52] CSD manages the ICS-CERT[53] and coordinates activities of the Industrial Control Systems Joint Working group (ICSJWG)[54]

6.1.2.2 National Protection and Programs Directorate, Office of Infrastructure Protection

"The Office of Infrastructure Protection leads the coordinated national effort to reduce risk to our critical infrastructure posed by acts of terrorism. In doing so, the Department increases the nation's level of preparedness and the ability to respond and quickly recover in the event of an attack, natural disaster, or other emergency."[55]

6.1.2.3 Science and Technology Directorate, Borders and Maritime Security Division

The Borders and Maritime Security Division works to enhance U.S. air, land and maritime border security through the transition of scientific and technical knowledge and solutions to operational use, while maximizing the flow of commerce and travel. Its primary customers are other operating components within DHS (Customs and Border Protection, Immigration and Customs Enforcement and the U.S. Coast Guard) and the nation's First Responders.[56]

6.1.2.4 Science and Technology Directorate, Infrastructure Protection and Disaster Management Division

The Infrastructure Protection and Disaster Management Division's mission is to "…advance national preparedness by improving and increasing the nation's strategic preparedness response to natural and man-made threats through superior situational awareness, emergency response capabilities and critical infrastructure protection."[57]

[52] Department of Homeland Security website, accessed May 1, 2013, https://www.dhs.gov/st-csd.
[53] Ibid, accessed May 1, 2013, https://ics-cert.us-cert.gov/.
[54] Ibid, accessed May 1, 2013, https://ics-cert.us-cert.gov/icsjwg/.
[55] Ibid, accessed May 1, 2013, http://www.dhs.gov/about-national-protection-and-programs-directorate.
[56] Ibid, accessed May 1, 2013, http://www.dhs.gov/st-bmd.
[57] Ibid, accessed May 1, 2013, http://www.dhs.gov/st-idd.

6.1.2.5 Transportation Security Administration

The Transportation Security Administration (TSA) was created following the attacks of September 11, 2001 to strengthen the security of the nation's transportation systems and ensure the freedom of movement for people and commerce. The TSA Office of Security Policy and Industry Engagement leads the unified national effort to protect and secure our nation's intermodal transportation systems, ensuring the safe movement of passengers and promotes the free flow of commerce by building a resilient, robust, and sustainable network with our public and private sector partners.[58] TSA has initiated several awareness and outreach activities that facilitate interaction with the transportation industry to exchange information on cyber security.

6.1.2.6 United States Coast Guard

As an operational element of the DHS, the USCG is well-positioned to access the broad resources of DHS and apply them to the maritime transportation system. The USCG has eleven mission functions established under law, regulation and policy; three of these functions have direct overlap with maritime cybersecurity issues:[59]

- Ports and waterway security and management
- Maintains aids to navigation and waterway management
- Marine safety, including vessel inspection and mariner certification

USCG Cyber Command (CG-6) is responsible for command, control, communications, computers and information technology (C4&IT) within the USCG, and supports both USCG-centric and DHS-wide efforts to address cybersecurity issues the maritime domain, particularly awareness, coordination, and unity of effort.[60]

[58] Transportation Security Administration website, accessed May 1, 2013, http://www.tsa.gov/stakeholders/intermodal-transportation-systems.

[59] United States Coast Guard website, accessed May 1, 2013, http://www.uscg.mil/top/missions/.

[60] United States Coast Guard Command, Control, Communications, Computers and Information Technology Strategic Plan, FY2013-FY2017, accessed May 1, 2013, http://www.uscg.mil/hq/cg6/docs/C4IT_Strategic_Plan_FY13-17.pdf.

6.1.3 DEPARTMENT OF DEFENSE

The Department of Defense (DoD) operates the world's largest global supply chain. DoD moves billions of dollars' worth of millions of different items across the U.S. and around the globe, to thousands of bases and installations, covering tens of millions of miles every year. National security requirements demand that these cargoes travel through a safe, secure, efficient and resilient supply chain. DoD relies predominantly upon non-Federal assets and infrastructure to move its cargo, making them an essential partner in transportation infrastructure security and resilience in the private sector. U.S.TRANSCOM relies on its commercial partners to meet 88 percent of continental U.S. land transport, 50 percent of global air movement, and 64 percent of global sealift.[61] In the military's maritime domain, two key stakeholders stand out:

6.1.3.1 U.S. Transportation Command / Military Sealift Command

The U.S. Transportation Command (U.S.TRANSCOM) is a joint DoD command responsible for all military transportation and logistics processes operations. U.S.TRANSCOM oversees the strategic highway and rail networks, planning strategic deployments and providing transit visibility of military freight movements.

Military Sealift Command (MSC) is the maritime component command of U.S.TRANSCOM, and operates over 100 noncombatant, civilian crewed vessels that move military cargo in support of military operations around the globe. This makes MSC the largest operator of U.S. flagged, oceangoing vessels, giving it a critical stake in ICS security. The MSC fleet is comprised of government-owned ships specifically designed for military support operations, as well as suitable, privately owned vessels under long-term charter. This joint ownership / operational structure represents a potential risk when addressing ICS control system vulnerabilities.

6.1.3.2 U.S. Army Corps of Engineers

The U.S. Army Corps of Engineers (U.S.ACE) is responsible for maintaining and operating the nation's inland waterway system, including 25,000 miles of channels, 236 lock chambers and 925 coastal, Great Lakes and inland harbors. Maintaining these waterways is critical to the safety, security and resilience of the Marine Transportation System. U.S.ACE also administers two other programs which pose potential threats to the maritime transportation system: levees (U.S.ACE maintains 14,400 miles of the nation's 100,000 miles of levees, some of which serve to create navigational channels while protecting adjacent low-lying land) and dams (U.S.ACE manages 694 dams, many of which impact water levels in downstream waterways).[62]

[61] U.S. Transportation Command website, accessed May 1, 2013, http://www.transcom.mil/about/whatIs.cfm.
[62] U.S. Army Corps of Engineers website, accessed May 1, 2013, http://www.usace.army.mil/Missions/CivilWorks.aspx.

6.2 Non-Federal Partners

PPD-21 directs the Federal Government to team up with the private sector to address risks and vulnerabilities of infrastructure security and resiliency. This partnership is critical since the vast majority of physical components making up the maritime transportation system – as with other transportation modes – are owned, operated or maintained by non-federal stakeholders. Three key stakeholder communities stand out as critical partners in this effort:

- Vessel owners and operators…to address and mitigate risks in existing shipboard systems.
- Port and terminal owners and operators…to address and mitigate risks of systems deployed ashore.
- Classification societies…to develop appropriate standards for vessel cybersecurity and security of control systems aboard ship.

These three groups are well represented by the following entities:

6.2.1 Chamber of Shipping of America

The Chamber of Shipping of America (CSA) was established in 1969 to represent the interests of U.S.-flag ship owners and operators in U.S. and international legislative, regulatory and administrative matters. It currently represents 35 companies, making it the largest of a small handful of industry advocacy organizations. CSA itself is a member of the International Chamber of Shipping, which represents national shipowner associations of 36 countries.[63]

Beyond its advocacy roles, the CSA seeks to, "Provide strong technical expertise, marine experience and knowledge, in order to be an authoritative and effective forum for U.S. maritime issues."[64] CSA is well-positioned to assist in bringing together management, operations and design personnel from the private sector, to work on maritime-related security activities.

6.2.2 American Association of Port Authorities

The American Association of Port Authorities (AAPA) would be a valuable partner in the ICS security effort. AAPA was founded in 1912 and represents more than 130 public port authorities in the United States, Canada, the Caribbean and Latin America. One of its objectives is, "…advocating issues critical to public seaports."[65]

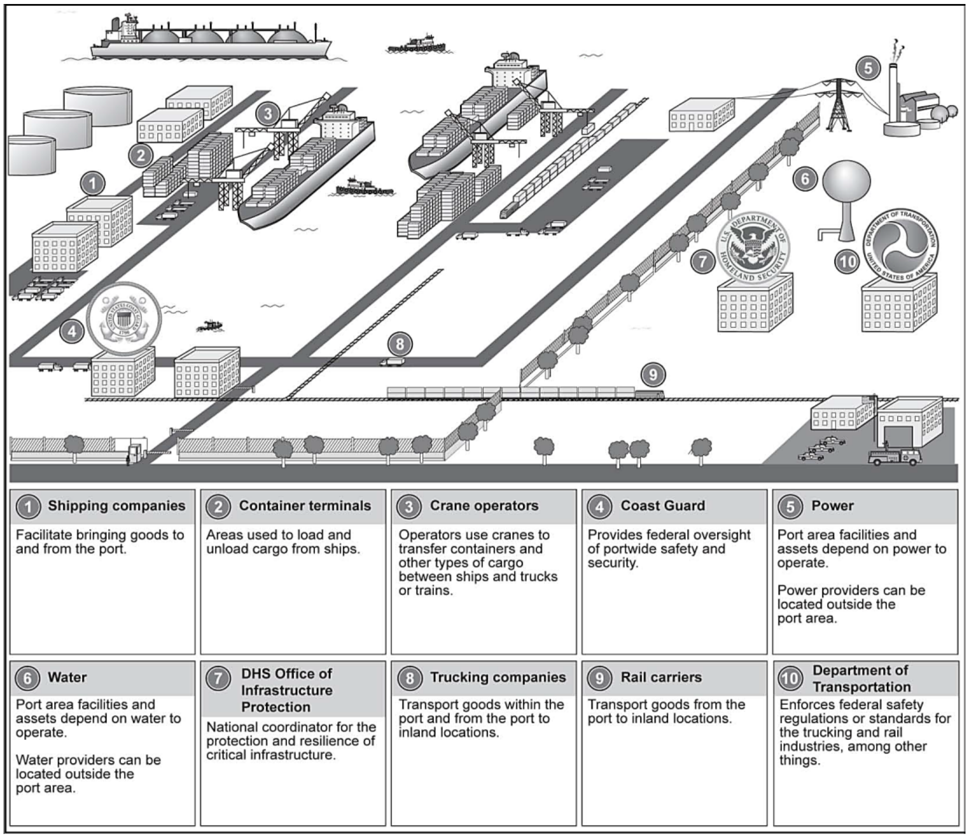
Port authorities are responsible for managing the overall safety, security and efficiency of the cargo and freight infrastructure in their charge. As public agencies, they also have close working

[63] Chamber of Shipping of America website, accessed May 1, 2013, http://www.knowships.org/.
[64] Chamber of Shipping of America website, accessed May 1, 2013, http://www.knowships.org/about.php.
[65] American Association of Port Authorities website, accessed May 1, 2013, http://www.aapa-ports.org/About/?navItemNumber=495.

relationships with their local stakeholders and representatives of federal agencies:

- Individual municipalities and states and their respective transportation departments, emergency management agencies, economic development councils, National Guard, etc.
- Federal agencies such as USCG, Environmental Protection Agency, Customs and Border Patrol.
- Cargo terminal operators (cargo terminals, container yards, passenger terminals, etc.)
- Modal transportation operators (vessel operators, rail carriers, motor carriers)

Figure 5 represents some of the overlapping government, municipal and private-sector stakeholders involved in port operation and security.



1 Shipping companies Facilitate bringing goods to and from the port.	2 Container terminals Areas used to load and unload cargo from ships.	3 Crane operators Operators use cranes to transfer containers and other types of cargo between ships and trucks or trains.	4 Coast Guard Provides federal oversight of portwide safety and security.	5 Power Port area facilities and assets depend on power to operate. Power providers can be located outside the port area.
6 Water Port area facilities and assets depend on water to operate. Water providers can be located outside the port area.	7 DHS Office of Infrastructure Protection National coordinator for the protection and resilience of critical infrastructure.	8 Trucking companies Transport goods within the port and from the port to inland locations.	9 Rail carriers Transport goods from the port to inland locations.	10 Department of Transportation Enforces federal safety regulations or standards for the trucking and rail industries, among other things.

Figure 5: Government, Municipal and Private-Sector Security Stakeholders

6.2.3 American Bureau of Shipping

Since the American Bureau of Shipping (ABS) was established in 1862, it has established itself as a respected, independent voice in matters regarding vessel design and construction. ABS publishes technical standards for the construction and periodic survey of vessels and has expanded its portfolio to include the evaluation, assessment and certification of vessels, companies and facilities for compliance with a wide variety of internationally recognized standards regarding safety, security and management.

ABS is the third largest classification society in the world, representing over 10,000 vessels registered in the U.S., as well as in many other nations.

Under 46 U.S. Code §3316, the ABS is granted exclusive jurisdiction as the Federal Government's agent in classifying vessels owned by the Government and in matters related to classification. When paired with their experience in the private sector, ABS is in a unique position to work with U.S. Government agencies such as MARAD and the Volpe Center to develop technical standards and implementation strategies for shipboard industrial control system security.

6.2.4 Other Industry Leaders

The MTS is comprised of a wide variety of public, quasi-public and private sector agencies and commercial operators. The latter two groups represent the largest number of MTS stakeholders. Consequently there may be other private sector corporations or organizations interested in taking a leadership role in developing, promulgating, and implementing industry best practices. Their motivation in ICS security is two-fold:

- Economic: Taking the necessary steps to mitigate operational disruptions to reduce risk is a fundamental management decision. Ensuring resilience is an industry best-practice, and fosters consumer confidence and loyalty.
- Regulatory: Ensuring the safe and secure flow of cargo, as well as protecting the associated physical, financial, and personnel transactions and movements, is required by the federal agencies responsible for transportation and commerce, e.g. Immigration and Customs Enforcement (ICE), TSA, USCG, etc.

7. Findings and Recommendations

7.1 Findings

1. The maritime transportation system is central to national security and economic stability. The majority of freight arriving and departing from the U.S. travels by ship.
2. Disruptions to the maritime transportation system impact the local, regional and national economies. The impact of an oil tanker grounded in a channel or a container terminal paralyzed by inoperative equipment will be felt throughout the supply chain.
3. Vulnerabilities exist in industrial control systems. These vulnerabilities can be exploited by accessing systems through public and private IT infrastructures, or through other means such as direct access to control devices.
4. There is no strong advocate for Industrial Control System Security in the global maritime transportation community. This finding is echoed by a 2011 report by the European Network and Information Security Agency that stated, "…awareness on cyber security needs and challenges in the maritime sector is currently low to non-existent."[66]
5. Opportunities for leadership exist. Changes in federal policy now give DOT greater responsibility for critical transportation infrastructure security and resiliency. This provides an opportunity for MARAD to engage in maritime control system security.
6. Some efforts are currently underway to address control system security. These initiatives primarily focus on other transportation modes or infrastructures and do not address many of the unique, interdependent aspects of maritime transportation.
7. Expertise is available. Expertise exists at the federal level (the Volpe Center, and various operational units of DHS) to address the technical issues and to develop implementation plans which mitigate risks.
8. A framework already exists to address control system vulnerabilities. The DHS National Cyber Security Division (NCSD) recently funded the Volpe Center to address ICS security in the transportation sector. Working with stakeholders across all modes, the team developed a "Roadmap to Secure Control Systems in the Transportation Sector" (the Roadmap) (see Appendix 1). This document joins plans developed for other critical infrastructures identified in PPD-21 and established a high-level set of goals, objectives and milestones aimed at mitigating cybersecurity risks.

[66] "Analysis of Cyber Security Aspects in the Maritime Sector". Heraklion, Crete: European Network and Information Security Agency, 2011, accessed May 1, 2013, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts.

7.2 Recommendations

1. Designate a lead agency within DOT responsible for addressing maritime control system security.

PPD-21 vests new authority and responsibility in DOT for addressing transportation system security. As DOT's maritime modal agency, MARAD could take on this leadership role on behalf of DOT. Specific recommendations to achieve this objective include the following:

a. Promote awareness of ICS security issues amongst US-flag ship owners and operators. MARAD's authority as a promotional agency allows it to "…[collaborate] extensively with stakeholders from all transportation sectors and modes in order to accomplish its mission to improve and strengthen the U.S. marine transportation system."[67] In this role, MARAD has a long history of working closely with the private sector on a wide variety of regulatory and operational issues. Its staff understands the maritime transportation business and understands federal laws and regulation. This experience gives MARAD the ability to effectively moderate discussions between regulators and operators and to identify solutions that implement federal policy in a responsible, cost-effective manner.

b. Fund research and implementation efforts. MARAD is authorized to "[conduct] research and development to improve and promote the waterborne commerce of the U.S."[68]

> *MARAD can utilize the resources of the Volpe Center to address ICS and other cybersecurity vulnerabilities of the MTS. The Volpe Center has the technical knowledge to address ICS security in a comprehensive, cross-modal manner, as well as the experience in working with other Federal agencies to implement transportation sector roadmaps and action plans. The Volpe Center is also well positioned to assist MARAD to address other maritime transportation cybersecurity vulnerabilities, such as GPS, since Volpe has experience in addressing identical issues in other modes that utilize GPS technology.*

c. Support activities of the DOT Safety Council Cyber Security Action Team (CSAT). MARAD represents the interests of the maritime community on the CSAT, and can ensure that CSAT recommendations are promoted throughout MARAD and the maritime community. Current recommendations include improving response capabilities to cyber incidents and incorporating cyber security in safety management plans.

d. Actively collaborate with other entities responsible for coordinating maritime transportation system safety, security and resilience. These include the USCG Cyber Command, Maritime Sector Coordinating Council (MSCC), Maritime Modal Government Coordinating Council (MMGCC), Area Maritime Security Committees (AMSC), and other local, regional, or industry groups.

[67] Title 49 U.S. Code: Subtitle A, Part 1, Subpart D, §1.92(g)
[68] Ibid

2. Implement the Department of Homeland Security's "Roadmap to Secure Control Systems in the Transportation Sector" and NIST 800-82.

The DHS NCSD recently funded the development of a plan to address ICS security in the transportation sector. Working with stakeholders across all modes, the Volpe Center team developed a "Roadmap to Secure Control Systems in the Transportation Sector" (the Roadmap). The Roadmap established a high-level set of short-, medium-, and long-term goals, objectives and milestones aimed at mitigating cybersecurity risks in the Transportation Sector. The four major goal areas are listed below; further information is found in Appendix 1.

- 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.

In May 2013, NIST updated Special Publication 800-82, a "Guide to Industrial Control Systems (ICS) Security". The NIST publication provides a comprehensive strategy and practical solutions for government and private sector agencies to use in implementing an ICS Security Program.

> *The Volpe Center is available to assist MARAD in this effort. Volpe's status as a federal agency gives the maritime transportation community access to expertise and materials not readily available to other entities. Volpe Center technical experts have significant experience addressing cyber- and ICS security, and are currently working with several other federal modal transportation agencies to assist them in developing solutions and strategies to mitigate their cybersecurity risks.*
>
> *In addition to assisting in development of the Roadmap, Volpe Center experts also served on the ICSJWG that produced the "Cross-Sector Roadmap to Secure Control Systems" in September 2011.*[69] *The ICSJWG is comprised of stakeholders in government, academia, owner/operators, system integrators and the vendor community and facilitated their collaboration to accelerate the design, development and deployment of more secure control systems.*

[69] "Cross-Sector Roadmap for Cybersecurity of Control Systems." Washington: Department of Homeland Security, September 2011, accessed May 1, 2013, http://ics-cert.us-cert.gov/pdf/Cross-Sector_Roadmap_9-30.pdf.

3. Ensure that ICS security and other maritime cybersecurity risks are considered in the implementation of MAP-21.

The “Moving Ahead for Progress in the 21st Century Act” (MAP-21) established a general framework for a national freight policy, and directed the Secretary of Transportation to develop a National Freight Strategic Plan in support of that policy.[70] Any National Freight Strategic Plan will identify maritime freight transportation solutions, and must also address cybersecurity risks. This will ensure that the National Freight Strategic Plan also complies with existing Federal requirements governing preparedness and critical infrastructure safety, security and resiliency.

Two entities have been created to guide the development of the National Freight Strategic Plan. An internal DOT Freight Policy Council, led by the Deputy Secretary, is comprised of the modal deputy administrators and other key DOT leaders.[71] An external advisory group, the National Freight Advisory Committee, was appointed in May, 2013.[72] These two groups will need technical support to ensure that their evaluation and subsequent recommendations address cybersecurity and resilience.

> *The Volpe Center is well positioned to assist this effort. Its multi-disciplinary expertise can assess risk and identify technical and operational solutions, in order to better inform policy decision makers.*

4. Ensure that ICS security and other maritime cybersecurity risks are considered in the implementation of the research provisions of PPD-21.

PPD-21 requires the development of a National Critical Infrastructure Security and Resilience R&D Plan:

> *Within 2 years of the date of this directive, the Secretary of Homeland Security, in coordination with the OSTP, the SSAs, DOC, and other Federal departments and agencies, shall provide to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a National Critical Infrastructure Security and Resilience R&D Plan that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments.*[73]

Such a plan must address maritime cybersecurity risks.

> *The technical expertise and thought leadership of the Volpe Center can be valuable assets in developing and executing such a plan. Their demonstrated experience across all transportation modes can assist MTS stakeholders in address inherent and dynamic infrastructure resilience.*

[70] 23 U.S. Code §167, accessed May 1, 2013, http://www.gpo.gov/fdsys/pkg/BILLS-112hr4348enr/pdf/BILLS-112hr4348enr.pdf.
[71] U.S. Department of Transportation, Freight Policy Council Charter, accessed May 1, 2013, http://www.dot.gov/sites/dot.dev/files/docs/DOT%20Freight%20Policy%20Council%20Charter.pdf.
[72] U.S. Department of Transportation, Freight Policy Advisory Committee announcement, accessed May 1, 2013, http://www.dot.gov/briefing-room/us-transportation-secretary-lahood-announces-national-freight-advisory-committee.
[73] Presidential Policy Directive 21.

5. Consider establishing a Critical Infrastructure Partnership Advisory Council (CIPAC) Maritime Transportation Sector Subcommittee

HSA 2002 authorized DHS to establish various committees and councils to coordinate the activities of government and private-sector stakeholders operating in each critical infrastructure sector.[74] These include "sector coordinating councils" (SCC), industry-focused partnerships that provide centralized, focused coordination with the government, and "government coordinating councils" (GCC) that are intended to enable interagency and cross-jurisdictional coordination.[75]

HSA 2002 also authorized the establishment of a Critical Infrastructure Partnership Advisory Council (CIPAC): "…to facilitate effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial and tribal governments. The CIPAC represents a partnership between government and critical infrastructure owners and operators and provides a forum in which they can engage in a broad spectrum of activities to support and coordinate critical infrastructure protection."[76]

Unlike the SCC and GCC, the CIPAC brings together government and private stakeholders to one forum. While there is a CIPAC Transportation Systems Sector Committee (which itself includes a Cybersecurity Working Group), and several modal-specific subcommittees, there are no CIPAC committees focused on the complexities and unique characteristics of the maritime transportation sector.

Establishing a CIPAC Maritime Transportation Sector Subcommittee might also address concerns expressed by the GAO in its 2012 report, "Critical Infrastructure Protection: An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts across Ports and Other Infrastructure".[77] That report contained the following recommendations:

> *To better ensure consistent implementation of and accountability for DHS's resilience policy, we recommend that the Secretary of Homeland Security direct the Assistant Secretary for Policy to develop an implementation strategy for this new policy that identifies the following characteristics and others that may be deemed appropriate:*
>
> *steps needed to achieve results, by developing priorities, milestones and performance measures;*
>
> *responsible entities, their roles compared with those of others and mechanisms needed for successful coordination; and*

[74] Department of Homeland Security website, accessed May 1, 2013, http://www.dhs.gov/critical-infrastructure-sector-partnerships.

[75] Both a Maritime Sector Coordinating Council (MSCC) and a Maritime Modal Government Coordinating Council (MMGCC) appear to exist, but there is limited information available as to past activities, recommendations or engagement.

[76] DHS website, accessed May 1, 2013, http://www.dhs.gov/critical-infrastructure-partnership-advisory-council.

[77] "Critical Infrastructure Protection: An Implementation Strategy Could Advance DHS's Coordination of Resilience Efforts across Ports and Other Infrastructure." Washington: Government Accountability Office, October 2012, accessed May 1, 2013, http://www.gao.gov/assets/650/649705.pdf.

> *sources and types of resources and investments associated with the strategy and where those resources and investments should be targeted.*
>
> *To allow for more efficient efforts to assess portwide resilience, the Secretary of Homeland Security should direct the Assistant Secretary of Infrastructure Protection [IP] and the Commandant of the Coast Guard to look for opportunities to collaborate to leverage existing tools and resources to conduct assessments of portwide resilience. In developing this approach, DHS should consider the use of data gathered through IP's voluntary assessments of port area critical infrastructure or [regional resiliency] assessments—taking into consideration the need to protect information collected voluntarily—as well as Coast Guard data gathered through its [Maritime Security Risk Analysis Model] assessments and other tools used by the Coast Guard.*

Notional membership of such a group is shown in Table 7.2.5.

Table 7.2.5: Notional Membership of a Maritime Transportation CIPAC

FEDERAL AGENCIES	NON-FEDERAL AGENCIES
• Department of Transportation o Office of the Secretary of Transportation o Maritime Administration o Saint Lawrence Seaway Development Corporation o Volpe National Transportation Systems Center • Department of Homeland Security o U.S. Coast Guard ▪ Cyber Command (C4IT) (CG-6) ▪ Office of Design and Engineering Standards (CG-ENG) ▪ Office of Port and Facility Compliance (CG-FAC) ▪ Director of Marine Transportation Systems (CG-5PW) o Office of Infrastructure Protection o Transportation Security Administration • Department of Defense o Military Sealift Command o o Army Corps of Engineers	• American Association of Port Authorities (AAPA) • American Bureau of Shipping (ABS) • Chamber of Shipping of America (CSA) • Cruise Line International Association (CLIA) • National Council of Information Sharing and Analysis Centers (ISACs) • Passenger Vessel Association (PVA) • Society of Naval Architects and Marine Engineers (SNAME) • World Shipping Council (WSC)

Some of these agencies may already interact through other forums and structures.

Appendix A

“Roadmap to Secure Control Systems in the Transportation Sector”
Goals, Objectives, Milestones and Metrics

	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.	a. The organization has a documented ICS cybersecurity business case.
	b. Identify roles and responsibilities, structure and authorities for ICS cybersecurity planning and risk management.	b. Personnel have been formally assigned ICS cybersecurity planning and risk management responsibilities and budgets.
	c. Educate transportation executives on the importance of ICS cybersecurity.	c. Many transportation executives recognize ICS cybersecurity as mission critical.
	d. Establish ICS cybersecurity policies and procedures, resources and budget/funding.	d. The organization has identified the ICS policies and procedures it will follow and has established the necessary ICS resources and budget/funding.
	e. Develop a cybersecurity awareness training program and begin delivering it to new hires and existing employees.	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.	a. The organization has further developed its cybersecurity awareness training program and has provided the training to many of its employees.
	b. Institutionalize cybersecurity language & methodologies in ICS contracts, user agreements, statements of work, asset mgmnt procedures, etc.	b. Most ICS-related procurements, documents, procedures and policies include provisions for cybersecurity.
	c. Develop a robust ICS self-assessment program/business case.	c. Asset owners and operators perform self-assessments of most of their ICS according to the frequency identified in their associated program/business case.
	d. Develop security assessment capabilities for new and legacy ICS.	d. The organization identifies its current security assessment capabilities for new and legacy ICS, including the types of assessment tools utilized.
	e. Establish a mechanism that allows for frequent and ongoing collaboration between operations and security cyber staff and ICS operators and engineers.	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 ICS.	a. Most ICS are continuously monitored via established automated processes.
	b. Ensure that cybersecurity awareness training is periodically updated and provided to personnel at all organizational levels.	b. The organization has an established process for updating its cybersecurity awareness training, with most staff receiving annual cybersecurity awareness refresher training.
	c. Incorporate cybersecurity language, reviews and considerations into all levels of ICS-related business practices and budgetary considerations.	c. Cybersecurity is integrated into most ICS business practices.
	d. Establish ISACs (or equivalent) for each transportation mode and for the Transportation Sector.	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.	a. Each organization identifies the risk management framework and standards it will follow.
	b. Identify common metrics for benchmarking ICS risk (threats-vulnerabilities-consequences).	b. Each organization prioritizes its identified ICS cybersecurity risks based on defined common metrics.
	c. Integrate cybersecurity into business functions and operation plans.	c. All business functions and operation plans contain a cybersecurity component.
	d. Develop and disseminate ICS risk assessment and reporting standards and guidelines that enable cybersecurity tools and metrics to be effectively deployed.	d. ICS risk assessment and reporting guidelines are published and disseminated throughout each organization.
	e. Identify cybersecurity risk management roles and responsibilities, including establishing authorities responsible for accepting and mitigating cybersecurity risk.	e. All asset owners and operators have identified personnel responsible for ICS cybersecurity risk management.
	f. Adopt and deploy cybersecurity posture assessment tools (Cybersecurity Evaluation Tool (CSET) or equivalent) for ICS cybersecurity vulnerability assessments.	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.	a. Each organization identifies the risk management model and strategy it will use.
	b. Develop and implement a risk assessment program, with considerations for both top-down and bottom-up approaches.	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. Examine and test the use of automated tool options for ICS.	c. Most owners and operator have examined and tested the use of automated tool options for ICS.
	d. Examine and assess real-time security assessment capabilities for new and, where appropriate, legacy systems.	d. Real-time security assessment capabilities have been reviewed for most ICS (new and legacy).
	e. Develop and implement a cyber risk management training program for personnel with cybersecurity responsibilities.	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.	a. Each organization has established a formal risk management program, including related processes, for risk measurement and reporting.
	b. Establish and implement a continuous and automated risk monitoring program, including tools, for ICS.	b. Most asset owners and operators are using continuous and automated ICS risk monitoring programs and tools.
	c. Incorporate risk management considerations into all levels of ICS cybersecurity (contracts, user agreements, purchases, etc.).	c. Cybersecurity is integrated into most ICS business practices.
	d. Establish and regularly use, communication mechanisms for measuring risk management performance and benchmarking among the transportation modes and with other sectors.	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. Develop and implement a cybersecurity ICS training program review process.	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.	a. ICS protection guidelines have been developed and disseminated throughout the organization.
	b. Develop a template protocol for responding to cyber incidents.	b. Many asset owners and operators have developed and implemented cyber incident response protocols.
	c. Establish mechanisms for sharing information between asset owners, operators and vendors to develop improved protection tools.	c. Each organization has established a process for sharing cybersecurity protection information among asset owners, operators and vendors.
	d. Identify, implement and maintain, where appropriate, existing built-in cybersecurity features in ICS equipment.	d. Most asset owners and operators have identified cybersecurity features built into their control systems and many have implemented these features, where appropriate.
	e. Encourage/prioritize that ICS vendors begin implementing or improving their equipment's cybersecurity features.	e. Each organization has established a preference for vendors offering equipment with enhanced cybersecurity features.
	f. Develop, implement and maintain cybersecurity measures, such as firewalls, intrusion detection, anti-virus protection, passcodes and patching technologies—having minimum host impact and without compromising safety.	f. Some asset owners and operators have begun implementing enhanced cybersecurity measures.
	g. Train employees on the ICS protection guidelines.	g. Most organizations have trained their employees on their ICS protection guidelines.
	h. Analyze the organization's current cybersecurity posture with respect to its compatibility with existing and new technologies.	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.	a. Each organization has reduced avg. patch installation time.
	b. Develop provisions for accommodating restarts in control systems design.	b. Each organization has established provisions for accommodating control system restarts at the design level.
	c. Implement and maintain effective ICS cybersecurity protection tools.	c. Each organization has implemented and is maintaining effective cybersecurity protection tools for ICS.
	d. Secure most of the interfaces between ICS and internal and external systems.	d. Asset owners and operators have established secure interfaces between most 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 ICS.	e. Many operators have completed a cybersecurity training program that includes information on the protection tools and features used to secure ICS.
	f. Perform nondisruptive intrusion tests on ICS to demonstrate the effectiveness of automated isolation and response mechanisms.	f. Many asset owners and operators have performed nondisruptive ICS intrusion tests.

(Long-term objectives for Goal 3 are found on the next page.)

	Goal 3 (Continued): Develop and Implement Risk Reduction and Mitigation Measures	
	Objectives	Milestones and Metrics
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.	a. Secure ICS architectures with built-in, end-to-end security are in all of the organization's critical ICS.
	b. Identify best practices for connecting ICS and business networks.	b. Each transportation mode has developed best practices for securely connecting ICS and business networks, where appropriate.
	c. Secure all of the interfaces between ICS and internal and external systems.	c. Asset owners and operators have established secure interfaces between all ICS and internal and external systems.
	d. Ensure that most operators receive specialized cybersecurity training commensurate with their respective duties and responsibilities.	d. Most operators have received ICS cybersecurity training commensurate with their respective duties and responsibilities.
	e. Encourage/prioritize that real-time monitoring tools for cybersecurity intrusions are commercially available.	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.	a. Some asset owners and operators have deployed sensors and systems for detecting and reporting abnormal ICS activity.
	b. Identify recommended practices and approved guidelines for incident reporting and information sharing of ICS cybersecurity-related events.	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. 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.	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. Develop and incorporate cyber incident response and recovery planning into established business continuity plans.	d. Some asset owners and operators have incorporated a cyber incident response and recovery planning component into their 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.	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. Work with vendors on specifications for new ICS detection and response tools and equipment.	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.	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. Establish procedures for the periodic upgrade of business continuity plans and training programs to reflect changes in new tools, equipment and recommended ICS practices.	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. 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.	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. Develop public communication strategies regarding the potential consequences of transportation network disruption from a cyber incident.	d. Each organization has developed public communication strategies for disseminating the potential transportation network disruption consequences resulting from a cyber incident.

(Long-term objectives for Goal 4 are found on the next page.)

	Goal 4 (Continued): Manage Incidents	
	Objectives	Milestones and Metrics
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.	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. Identify and implement real-time detection and response ICS tools and equipment in each mode and throughout the Transportation Sector.	b. Real-time ICS detection and response tools and equipment are present 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.	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.	

U.S. Department of Transportation
John A. Volpe National Transportation Systems Center
55 Broadway
Cambridge, MA 02142-1093

(617) 494-2000
www.volpe.dot.gov

DOT-VNTSC-MARAD-13-01