# TSA Surface Cybersecurity Resources

**Lee Allen**

*DHS/TSA/Office of Security Policy & Industry Engagement/Surface Division, Cybersecurity Lead*

*Arlington, VA*

# Key Presentation Take-Aways

- Cyber Critical Infrastructure Protection
- Cybersecurity Efforts and Resources
- Information Sharing and Working Groups
  - Get Involved

# Cyber Critical Infrastructure Protection

- **Mandates**
  - Executive Order 13636: Improving Critical Infrastructure Cybersecurity.
  - Presidential Policy Directive-21: Critical Infrastructure Security and Resilience.
  - Presidential Policy Directive-41: United States Cyber Incident Coordination.
  - Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- **Approach**
  - **Non-Operational**. Education, Facilitation, and Communication.

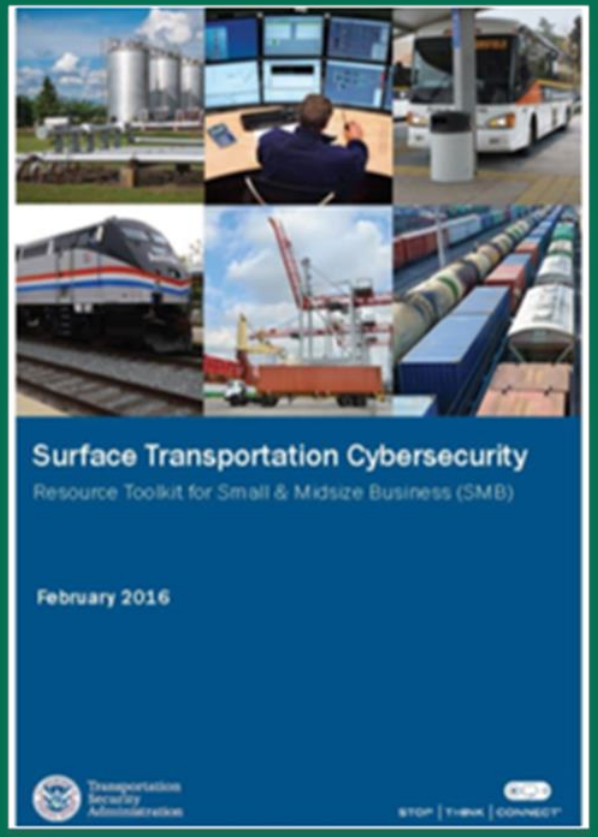
# Put Cybersecurity Risk Management on the Agenda Before it Becomes the Agenda

- No longer sufficient to think about cybersecurity as a purely technical problem.
- Like physical security, the current threat environment requires a comprehensive approach to cybersecurity risk management.
- It is vital to realize the importance of protecting your company's systems from cyber threats.

# Surface Division's Cybersecurity Efforts

- Collaboration with industry and government partners to promote cybersecurity risk management resources and programs through awareness and outreach.
- With the goal of:
  - Supporting the adoption of the Cybersecurity Framework.
  - Increasing an organization's operational resilience and ability to manage cyber risk.

# Surface Transportation Cybersecurity Resource Toolkit for Small & Midsize Business (SMB)




- Collection of resources and programs designed to offer guidance on how to incorporate “Cyber Risk” into your organization's existing risk management and governance processes.

# No Cost Resources for Surface TSS Industry Stakeholders

Transportation Security Administration

**Surface Transportation Cybersecurity**
Resource Toolkit for Small & Midsize Business (SMB)
No-Cost Cybersecurity Resource List

**American Public Transportation Association Cybersecurity Considerations for Public Transit:** This *Recommended Practice* establishes considerations for public transit chief information officers (CIOs) interested in developing cybersecurity strategies for their organizations. It details practices and standards that address vulnerability assessment and mitigation, system resiliency and redundancy, and disaster recovery. To download, visit: http://www.apta.com/resources/standards/Documents/APTA%20SS-ECS-RP-001-14%20RP.pdf

**American Public Transportation Association Securing Control and Communications Systems in Transit Environments:**

- **Part I: Elements, Organization and Risk Assessment/Management:** This *Recommended Practice* addresses the importance of control and communications security to a transit agency, provides a survey of the various systems that constitute typical transit control and communication systems, identifies the steps that an agency would follow to set up a successful program, and establishes the stages in conducting a risk assessment and managing risk. To download, visit: http://www.apta.com/resources/standards/Documents/APTA-SS-CCS-RP-001-10.pdf
- **Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones:** This *Recommended Practice* presents Defense-In-Depth as a recommended approach for securing rail communications and control systems, defines security zone classifications, and defines a minimum set of security controls for the most critical zones. To download, visit: http://www.apta.com/resources/standards/Documents/APTA-SS-CCS-RP-002-13.pdf
- **Part IIIa: Attack Modeling Security Analysis White Paper:** This *White Paper* covers the APTA attack modeling procedure for transit agencies and their systems integrators and vendors, which may be specified by transit agencies in their procurement documents. To download, visit: http://www.apta.com/resources/standards/Documents/APTA-SS-CO-03-15.pdf

**Pipeline Security Guidelines:** Provides security measures for cyber assets and a list of cybersecurity planning and implementation guidance resources. To download, visit: https://www.tsa.gov/sites/default/files/tsapipelinesecurityguidelines-2011.pdf

**Transportation System Sector Cyber Working Group (TSSCWG):** TSA sponsored public/private joint working group that provides a forum for implementing and facilitating national policies, programs, modal outreach, awareness, and information sharing. The group meets monthly and also published a weekly newsletter. To be invited, contact Cybersecurity@tsa.dhs.gov

**Public Transportation Information Sharing and Analysis Center (ISAC):** An electronic, trusted ability to exchange and share information on physical and cyber threats. The center collects, analyzes, and disseminates alerts and incident reports, as well as sector-specific intelligence products, and helps the government understand sector impacts. To request access to this free service, contact st-isac@surfacetransportationisac.org

**Stop.Think.Connect. Campaign:** National public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Includes customized awareness materials for industry, government, law enforcement, small business, and others. For more information, visit: http://www.dhs.gov/stopthinkconnect

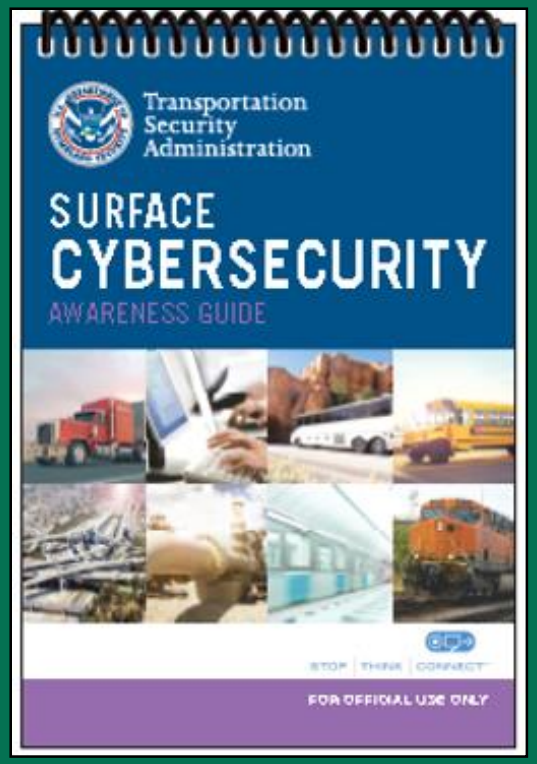
**Cybersecurity Framework (CSF):** Risk-based approach to managing cybersecurity risk, allowing framework components to reinforce the connection between business drivers and cybersecurity activities. The framework was developed to complement, not replace, an organization's established risk management process and cybersecurity program. For more information, visit: http://www.nist.gov/cyberframework/

- "No-Cost Cybersecurity Resources for Surface Transportation systems" is a factsheet that provides a list of cybersecurity programs and documents that industry can use to reduce their cybersecurity risk and increase their cyber resilience.

<u>Examples include:</u>

- The Critical Infrastructure Cyber Community Voluntary Program ($C^3VP$)
- Cyber Risk Management Primer for CEOs/Business Leaders
- Information about the Cyber Resilience Review (CRR) & Cyber Security Evaluation Tool (CSET)

# Surface Cybersecurity Awareness Guide




- Small “pocket-sized” guide outlines the types of threats most commonly found in cyberspace and explains how you can protect your company’s data, computer systems, and personal information.
- Serves as a convenient quick reference resource and security awareness tool for employees.

# Surface Division Cybersecurity Workshops


- Informs stakeholders about cybersecurity resources, programs and elicit feedback.
- Facilitate discussions of best practices and lessons learned associated with implementing cybersecurity measures.
- Multi-modal participants receive five nontechnical takeaways to consider over the next five days ("5 in 5") to enhance their transportation organizations' cybersecurity posture.

# Public Transportation Information Sharing & Analysis Center (PT-ISAC)

- Immediate “all source” incident reporting and threat warning.
- “Push” information vice members having to “Pull” information.
- Unique intelligence sources not normally available:
  - U.S. and foreign governments/International forums
  - National and International Computer Emergency Response Teams (CERTs)
  - Law enforcement entities
  - Independent research


ST-ISAC PT-ISAC

TRIAD

ST & PT ISACs Transit and Rail Intelligence Awareness Daily Report (TRIAD)

Friday, June 15, 2012

CYBER SECURITY

Daily Open Source Cyber Report

Executive and Technical News and Information

3 January 2017

- PT ISAC’s Transit and Rail Intelligence Awareness Daily Report (TRIAD)
- Daily Open source Cyber Report

# Transportation Systems Sector Cyber Working Group & Weekly Newsletter

This week in
Transportation Cybersecurity

Transportation Security Administration

Volume 7, Issue 46 | November 10, 2016

**Join us!**

Transportation Systems Sector Cyber Working Group Meeting (TSS-CWG)

23 November, 1-2 PM
Open to GCC and SCC Members

Interested?

Contact:
Cybersecurity@tsa.dhs.gov

**Airlines Shift Toward Smartphone IDs and Automation to Increase Efficiency**

Airports across the country continue to face new challenges. Social and technological advances have the potential to radically change current airline protocol. Identity management with airports is changing as states across the country are adopting a comprehensive digital identity solution for their citizens. Digital drivers licenses, e-passports, and other secure digital documents will make travel easier for many, but will also introduce additional challenges in authentication and the verification of travelers. Airlines must prepare for the challenges that lie ahead. Adopting a comprehensive digital solution to identity management is essential. The shift toward digital identity technology is not the only thing on the minds of airport executives. Congress held hearings this summer on the inefficiencies of airports security.

*Full Story:* http://www.aviationpros.com/article/12258141/airlines-shift-toward-smartphone-ids-and-automation-to-increase-efficiency

**Five Things Businesses Should Do For Cyber Security**

When I talk to CEOs across the country and ask them what keeps them up at night, inevitably one of the top three responses is related to cybersecurity concerns, and no wonder. With highly publicized data breaches (like Yahoo, Target, LinkedIn and J.P. Morgan), compliance requirements, and new state-specific laws requiring expensive disclosure situations, there is much to address. While most media attention has been focused on large companies, small- and medium-sized businesses are frequent targets as well. So what can business leaders realistically do to protect their organizations? Although some technical aspects of cybersecurity are very complex, the underlying concepts are relatively simple to grasp. Here are five steps businesses should take for a strong foundation in a cybersecurity strategy.

Know Your Sensitive Data: The first thing a business must do to begin a cybersecurity program is to identify what data it has. Once you have identified all the sensitive data that must be protected against unauthorized access, you need to focus on where it is located. How can you protect something if you don't know where it is? These locations can be desktops, laptops, servers, mobile devices and cloud providers, to name a few. Put this in the context of things in your home. You have perimeter protections such as locks and alarm systems for the items in your home. However, you know the items that are of higher value and may have a safe hidden somewhere for additional protection in the event of a break-in.

*Full Story:* http://www.knoxnews.com/story/money/business/journal/2016/11/07/5-things-businesses-should-do-cyber-security/92054284/

**Researchers Hijack Public Wi-Fi Connections To Track Cellphones**

One morning on the underground in London, Piers O'Hanlon, a privacy and security researcher at Oxford Internet Institute, noticed something strange about his phone: It kept automatically connecting to Wi-Fi networks from his provider without asking for a password displaying a small lock icon.

What started off as another morning on the tube prompted O'Hanlon's next research project. He began digging into the widely available public, automatic Wi-Fi provided by the phone companies, and looking at the ways it could be exploited and spied on. It turns out, those connections, which largely happen without consent, are insecure and unencrypted and can be easily intercepted by malicious hackers or law enforcement.

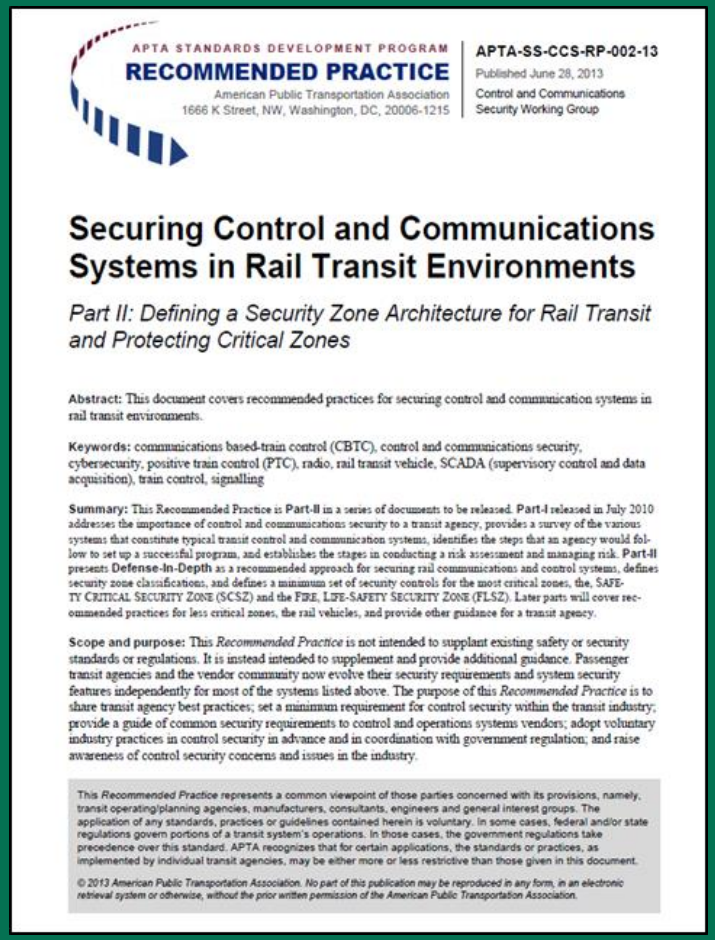
What O'Hanlon and his Oxford research associate, Ranjit Jankar Borgaonkar, looked into was a previously known but unaddressed flaw in the automatic Wi-Fi protocols that would allow someone to track the location of phones that connect to these networks. While tech experts are aware of the flaw, it's so deeply engrained in the system that it would require a large overhaul to fix, something companies aren't eager to invest in.

*Full Story:* https://theintercept.com/2016/11/07/hackers-and-law-enforcement-could-hijack-wifi-connections-to-track-cellphones/

- Joint Working Group
- Monthly Meetings
- Implementing National Policies
- Modal Outreach Awareness and Coordination
- Information Sharing Best Practices
- Facilitating Government Programs and Efforts
- Weekly Newsletter

# APTA Recommended Practice Cybersecurity Working Groups

- **Control and Communications Security**
  - Securing Control and Communications Systems in Transit Environments Part 1
  - Securing Control and Communications Systems in Rail Transit Environments Part 2
  - Securing Control and Communications Systems in Rail Transit Environments, Part 3a
  - Securing Control and Communications Systems in Rail Transit Environments Part 3b
- **Enterprise**
  - Cybersecurity Considerations for Public Transit



APTA STANDARDS DEVELOPMENT PROGRAM
RECOMMENDED PRACTICE
American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215

APTA-SS-CCS-RP-002-13
Published June 28, 2013
Control and Communications Security Working Group

## Securing Control and Communications Systems in Rail Transit Environments

*Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones*

**Abstract:** This document covers recommended practices for securing control and communication systems in rail transit environments.

**Keywords:** communications based-train control (CBTC), control and communications security, cybersecurity, positive train control (PTC), radio, rail transit vehicle, SCADA (supervisory control and data acquisition), train control, signalling

**Summary:** This Recommended Practice is Part-II in a series of documents to be released. Part-I released in July 2010 addresses the importance of control and communications security to a transit agency, provides a survey of the various systems that constitute typical transit control and communication systems, identifies the steps that an agency would follow to set up a successful program, and establishes the stages in conducting a risk assessment and managing risk. Part-II presents **Defense-In-Depth** as a recommended approach for securing rail communications and control systems, defines security zone classifications, and defines a minimum set of security controls for the most critical zones, the, SAFETY CRITICAL SECURITY ZONE (SCSZ) and the FIRE, LIFE-SAFETY SECURITY ZONE (FLSZ). Later parts will cover recommended practices for less critical zones, the rail vehicles, and provide other guidance for a transit agency.

**Scope and purpose:** This *Recommended Practice* is not intended to supplant existing safety or security standards or regulations. It is instead intended to supplement and provide additional guidance. Passenger transit agencies and the vendor community now evolve their security requirements and system security features independently for most of the systems listed above. The purpose of this *Recommended Practice* is to share transit agency best practices; set a minimum requirement for control security within the transit industry; provide a guide of common security requirements to control and operations systems vendors; adopt voluntary industry practices in control security in advance and in coordination with government regulation; and raise awareness of control security concerns and issues in the industry.

This *Recommended Practice* represents a common viewpoint of those parties concerned with its provisions, namely, transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any standards, practices or guidelines contained herein is voluntary. In some cases, federal and/or state regulations govern portions of a transit system's operations. In those cases, the government regulations take precedence over this standard. APTA recognizes that for certain applications, the standards or practices, as implemented by individual transit agencies, may be either more or less restrictive than those given in this document.

# TSA Surface Cybersecurity Resources

- For additional information and/or to request the *Awareness Guide* or *Toolkit*, email: Lee.Allen@tsa.dhs.gov

- For additional information about joining the Transportation Systems Sector Cyber Working Group or to receive *This Week in Transportation Cybersecurity*, email: Cybersecurity@tsa.dhs.gov