No-Cost Cybersecurity Resources for Surface Transportation Systems

- **American Public Transportation Association (APTA): 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

- **APTA: 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 system security 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-CC-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/pipeline_security_guidelines.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):** A trusted resource 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

- **Critical Infrastructure Cyber Community Voluntary Program (C³VP):** Supports critical infrastructure owners and operators interested in improving their cyber risk management processes and cyber resilience. Designed to increase awareness and use of the Cybersecurity Framework and to encourage organizations to manage cybersecurity as part of an all-hazards approach to enterprise risk management. For more information, visit: http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program and https://www.us-cert.gov/ccubedvp/smb

- **Cyber Risk Management Primer for CEOs:** Provides key cyber risk management concepts that business leaders should consider. Highlights the five questions business leaders should ask about cyber risks to protect their organization's systems from cyber threats. For more information, visit: http://www.dhs.gov/sites/default/files/publications/C3%20Voluntary%20Program%20-%20Cyber%20Risk%20Management%20Primer%20for%20CEOs%20_5.pdf

- **Industrial Control Systems (ICS) Cybersecurity for the C-Level:** Provides a tool to help facilitate the communication of strong cybersecurity principles to corporate leadership. Highlights the six questions business executives should be asking about their organization's Supervisory Control and Data Acquisition (SCADA) system/ICS. For more information, visit: https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_ICS_Cybersecurity_C-Level_S508C.pdf

- **Cyber Resilience Review (CRR) & Cyber Security Evaluation Tool (CSET):** These are DHS cyber risk assessments that are available as self-assessment downloads. They serve as a first step for organizations adopting the cybersecurity framework and explain how to manage cybersecurity risk. For more information, visit:
  https://www.us-cert.gov/sites/default/files/c3vp/crr-fact-sheet.pdf and
  https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_CSET_S508C.pdf

- **Law Enforcement Cybersecurity Resources:** Provides a list of DHS-recommended support materials for the law enforcement community. For more information, visit:
  http://www.dhs.gov/publication/stopthinkconnect-law-enforcement-resources
  - Law Enforcement and Cybersecurity
  - Law Enforcement Cyber Incident Reporting
  - Government Tip Card
  - DHS Cybersecurity Overview
  - DHS Federal Offerings
  - USSS Electronic Crimes Task Forces
  - Mobile Security Tip Card
  - Mobile Security One Pager
  - Cybersecurity While Traveling Tip Card
  - Internet of Things Tip Card
  - Stop.Think.Connect. Campaign Backgrounder

- **Cyber Incident Reporting:** info@us-cert.gov or (888)282-0870