Working Document of the NPC Study
Dynamic Delivery –
America's Evolving Oil and Natural Gas Transportation Infrastructure
Made Available December 12, 2019

Topic Paper #4-17

CYBERSECURITY CONSIDERATIONS RELATING TO RAIL TRANSPORTATION

Prepared for the

Technology Advancement and Deployment Task Group

On December 12, 2019 the National Petroleum Council (NPC) in approving its report, *Dynamic Delivery – America's Evolving Oil and Natural Gas Transportation Infrastructure*, also approved the making available of certain materials used in the study process, including detailed, specific subject matter papers prepared or used by the study's Permitting, Siting, and Community Engagement for Infrastructure Development Task Group. These Topic Papers were working documents that were part of the analyses that led to development of the summary results presented in the report's Executive Summary and Chapters.

These Topic Papers represent the views and conclusions of the authors. The National Petroleum Council has not endorsed or approved the statements and conclusions contained in these documents, but approved the publication of these materials as part of the study process.

The NPC believes that these papers will be of interest to the readers of the report and will help them better understand the results. These materials are being made available in the interest of transparency.

The attached paper is one of 26 such working documents used in the study analyses. Appendix C of the final NPC report provides a complete list of the 26 Topic Papers. The full papers can be viewed and downloaded from the report section of the NPC website (www.npc.org).

This page is intentionally left blank.

Topic Paper

(Prepared for the National Petroleum Council Study on Oil and Natural Gas Transportation Infrastructure)

4-17	Cybersecurity Considerations Relating to Rail Transportation
Author(s)	**Tom Farmer (Association of American Railroads)** **Rick Holmes (Union Pacific Railroad)**
Reviewers	**Al Lindseth (Plains All American)** **Marty Willhoite (Miller Consulting Services)** **Wesley Mallaby (Phillips 66 Company)** **Doug Sauer (Phillips 66 Company)** **Jay Churchill (Phillips 66 Company)**
Date: December 10, 2019	**Revision:** Final

SUMMARY

For security of information technology networks and systems and sustained safe and efficient train operations, America's major railroads have taken proactive and multi-faceted steps to prevent, respond to, and build resiliency against cyber threats. Implementing security programs guided by internationally recognized standards, railroads perform thorough assessments of potential vulnerabilities; implement protective countermeasures; and recruit and train specialized cybersecurity staff. Even the most effective cybersecurity plans and procedures will falter if useful information on cyber threats is not shared, which is why timely and comprehensive intelligence and information sharing between government security agencies and railroads is essential if cybersecurity efforts are to succeed.

I. OVERVIEW – RAIL

1. Overview

Freight railroads move vast amounts of products, commodities, and materials critical to Americans' health, quality of life, and economic well-being across the 140,000-plus mile rail network in the United States. Combined, the Class I railroads maintain (and annually inspect) more than 61,000 railroad bridges in the United States. For 2018, there were over 6 million total carloads hauled. The average train weighs more than 6,600 tons.

Most importantly, railroads transport these massive volumes at a fraction of the energy consumption and emissions of other means. If railroads didn't move freight in the United States, each day it would take over 120 million additional trucks traveling on public roadways, consuming four times the amount of fuel, to handle the freight. Moreover, the just over 600 railroads collectively maintain the 140,000 total route miles spread across 49 of the 50 states, the equivalent of 5.6 trips around the earth. The overwhelming majority of funding

to maintain and enhance infrastructure, and to construct new assets and facilities, comes from the railroads themselves – without taxpayer support.

Rail lines are comprised of the property and equipment of multiple operations, and potentially crosses multiple jurisdictions, with connections between multitudes of stakeholders. Security risk must be managed effectively throughout the network, both physical and cyber.

Interoperability is an essential capability for the railroad industry, as 60 percent of all rail cargo travels over lines owned by more than one railroad. This operational necessity is not, by any means, trivial. More than 500 railroads have to ensure that any other railroad's locomotives can safely travel over lines they own or maintain.

Railroads operate in all parts of the continental United States. There are rail lines that go through mountains, traverse deserts, as well as areas that experience annual flooding, tornadoes, hurricanes, and massive snow storms. Due to these varied and demanding topographical, climatological, and other factors, railroads have also had to leverage a broad array of communication technologies to support their operations as well, including radio, microwave, cellular, MPLS, and more.

2. Railroads and the Energy Sector

Rail transportation plays a substantial role in the Energy Sector's supply chain. While probably most widely recognized as the primary method of transport for coal, railroads also account for approximately 70% of ethanol movement in the United States. Each of the seven Class I railroads – five based in the United States and two in Canada with extensive operations and infrastructure in the United States – transport ethanol, with some serving several dozen plants. Furthermore, technological advances in shale oil extraction over the last decade have led to a surge in crude oil production in both countries.

Rail has been an essential transportation partner in ensuring the vast expansion in crude oil production reaches destinations for refining and export. In addition to transporting oil, condensate, and Natural Gas Liquids (NGLs), rail has also been vital in getting the sand and other drilling and extraction related products to the locations at which they are needed. These materials include: barite; bentonite clay; cement and rock; calcium chloride; guar; fracking tanks; crane and drilling mats; and supporting equipment and machinery.

3. Common Carrier / Handling of Hazardous Materials

Railroads are common carriers and, therefore, are required to transport flammable liquids, such as crude oil, natural gas, and butane; toxic inhalation hazard (TIH) materials, notably chlorine and anhydrous ammonia; and rail security-sensitive materials, or RSSM, which comprise hazardous materials determined by federal regulations administered by the United States Department of Transportation (DOT) and the Transportation Security Administration (TSA) to merit specific requirements for enhanced safety and security. TIH is included in the

scope of materials designated as RSSM. Collectively, these commodities are commonly referred to as "hazmat," the abbreviation for hazardous materials. Hazmat transport is subject to oversight by the Federal Railroad Administration (FRA), Pipeline and Hazardous Materials Safety Administration (PHMSA), the Department of Homeland Security (DHS), and TSA.

Railroads maintain an exceptional compliance record with federal regulatory requirements as well as agreed action items for safe and secure of hazmat generally and RSSM specifically. As representative examples, the collective railroad industry compliance rate with TSA requirements for secure transport and handling of RSSM consistently exceeds 99 percent – based on inspections conducted by the agency's surface transportation field teams. In similar vein, implementation of agreed security action items also consistently ranks in the 98 to 99 percent range cumulatively industry-wide.

Each year, pursuant to DOT regulation, railroads conduct thorough risk assessments of routes used to transport RSSM and flammable liquids, including crude oil, applying 27 distinct factors through the Rail Corridor Risk Management System (RCRMS), jointly developed by the federal government and the industry. Outreach to state and local government officials solicits input for the analysis. The results inform selection of safe and secure routes for transport of these materials. Further, railroads support preparedness of state and local emergency management officials and emergency responders, notably through hazmat and flammable liquids training initiatives, response exercises, and information sharing via two principal means – in response to requests, a delineation of all hazardous materials transported in a state or local jurisdiction; and the AskRail application, which enables emergency responders to obtain details on the consist of a train, notably any and all hazmat, by entry of a single rail car number, with links to response guides for specific hazardous commodities. Finally, railroads train their employees on special operating procedures to assure the safe and secure pick-up, movement, storage, and delivery of hazmat

On the latter point, railroads devote enormous resources to safe operations, no matter what they are hauling. The transport of hazmat revolves around three key areas: accident prevention; accident mitigation; and emergency response.

Accident **prevention** is always the primary objective. This objective has generally been accomplished by recurring physical inspections of locomotives, cars, and tracks by railroad employees. Increasingly, technology components are automating specific aspects of these inspections. Defect detectors, for example, are sensors that are normally integrated into the tracks for the purpose of detecting several different types of axle and signal problems in trains that pass over them. Similarly, hot-box detectors are sensors along the tracks that detect when axle bearings overheat. Besides detecting failures, improving safety systems is also important. As representative examples, this effort encompasses enhancements to train braking and use of assessment tools, such as the Rail Corridor Risk Management System cited above (to be described in more detail below), which enables completion of the route analyses for safety and security mandated by federal regulation.

Accident **mitigation** is a necessary accompanying priority, focusing on reducing the impact of any accidents that do occur. The main risk involved with an accident involving

hazardous materials is breach or compromise of the tank car or container, release of content, and exposure of railroad employees and of people who reside or work in the affected area. As a result, continuous and extensive effort is devoted to enhancing tank car safety and design standards.

Emergency **response** is the final area of focus, encompassing training, exercises, and information sharing to elevate preparedness of local first responders. Cumulatively, railroads have trained tens of thousands of responders each year throughout the country. The training ranges from general awareness to in-depth offerings. Several railroads use "hazmat safety trains" that travel from community to community to provide hands-on training to local first responders. In addition, several railroads operate centralized regional hazmat training sites where they train employees, first responders, customers, and other industry personnel. Railroads also visit hundreds of local firehouses each year, as well as regularly partner with local emergency responders to conduct simulations of emergency situations. Finally, technologies such as the "AskRail" app are made available to emergency responders to enable identifying the contents of railcars and provide emergency response information for the commodities contained.

Combining this emphasis on prevention, mitigation, and response with the industry's strong safety culture and use of safety-enhancing technologies, recent years have been the safest in rail history. Looking to the future, the freight rail industry will use today's technology as the foundation for even more innovation, to further enhance network safety and security.

II. OVERVIEW – RAIL TECHNOLOGIES

a. Train Control Systems

Train control system technologies and infrastructure support the safe operation of trains. They can be grouped into the following sets of technologies:

1. **Onboard Locomotive Systems** – provide automatic location tracking and reporting to the owning railroad's Transportation Control System (maintains real-time information about the block location of every train operating on the Company's track network, whether domestic or foreign), predictive enforcement braking, and automated transmission of movement authorities, switch monitoring, and control information.
2. **Field Systems** – provide remote monitoring and control of wayside devices by the dispatching system, locomotives, and track forces. Wayside devices include power- and hand-operated switches, railway crossings at grade, train defect detectors, and track integrity indicators.
3. **Central Dispatch System** – manage the movement of trains throughout the rail network with the objective of guaranteeing safe operations without incurring train delays. Much of the data relied upon is provided by the Field Systems. Crew Dispatchers rely

on this information when issuing track warrants, general orders, and other time-sensitive information to the locomotive crew. These systems enable efficient train movement, and rail fluidity would be significantly hampered in the event of a loss of dispatching systems.

4. **Crew Systems** – maintain information on availability, scheduling, and contact means to members of trains crews. Manual crew notification is a secondary option, though it is less efficient and relies upon underlying contact data that may be less readily available or accessible.

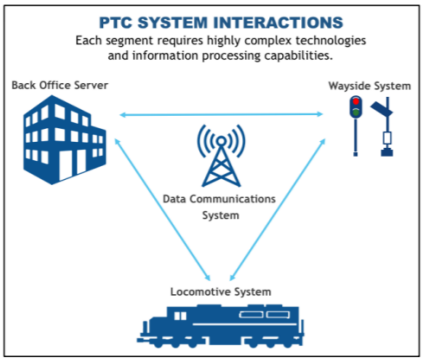
5. **Automated Systems and Hump Yards and Intermodal Facilities** – optimize operations by managing assembly of trains for deliveries of products, commodities, and materials to identified destinations and recipients.

III. POSITIVE TRAIN CONTROL OVERVIEW

Train operation safety is further enhanced through the development and deployment of positive train control technologies. The **Positive Train Control (PTC)** system is designed to **stop or slow a train automatically** in order to prevent potential accidents, caused by human error, including: train-to-train collisions, derailments caused by excessive speed, unauthorized incursions by trains onto sections of track where maintenance activities are underway, and the movement of a train through a track switch left in the wrong position.

A PTC system isn't conceptually that different from conventional train control systems, as it still consists of three main elements:

1. An onboard or locomotive system that monitors a train's position and speed and activates brakes as necessary to enforce speed restrictions and prevent unauthorized train movements;
2. A wayside system that monitors railroad track signals, switches, and track circuits to communicate data on this local infrastructure needed to permit the onboard system to authorize movement of a locomotive; and
3. A back-office server that stores all information related to the rail network and all trains operating across it (e.g., speed restrictions, movement authorities, train compositions, etc.); and transmits this information to individual locomotive onboard enforcement systems.



These three elements are integrated by a wireless data communications system that must move massive amounts of information back and forth between the back office servers, the wayside equipment, and the locomotive's on-board computers.

Class I freight railroads are committed to safely and fully implementing PTC as quickly as feasible. By the end of 2018, each Class I railroad met statutory requirements by having:

- Implemented PTC, or initiated revenue service demonstration, on at least 51 percent of its required PTC route-miles or subdivisions;
- 100 percent of PTC wayside, back office, and locomotive hardware installed;
- All required spectrum in place; and
- All required employee training completed.

In aggregate, Class I railroads had completed 83 percent of required PTC route-miles by the end of 2018 – or approximately 45,000 of the 54,000 route miles that must be equipped.

Class I railroads have been operating trains in PTC mode on much of their PTC routes as of the end of 2018. All will be fully operating their own trains in PTC mode on all their PTC routes no later than 2020, as required by federal law.

To work effectively, the PTC system must be able to determine the precise location, direction, and speed of trains; warn train operators of potential problems; and take immediate action if the operator fails to act after a warning from the PTC system. For example, if a train operator fails to begin stopping a train before a stop signal, the PTC system will apply the brakes automatically, before the train passes the stop signal.

Such a system requires highly complex technologies able to analyze and incorporate the huge number of variables that affect train operations. A simple example: how long it takes to stop a train depends on train speed, terrain, the weight and length of the train, the number and distribution of locomotives and freight cars on the train, and other factors. A PTC system must be able to take all these factors into account automatically, reliably, accurately, and in real time, in order to safely stop the train wherever it is along its route.

The secure design and implementation of PTC across all North American railroads was a monumental undertaking. It constituted an unprecedented challenge for the industry. Tasks that Class I freight railroads had to complete included:

- Physically surveying covered infrastructure and producing highly precise geo-mapping of the more than 54,000 route-miles on which PTC technology was installed, including more than 450,000 field assets along the right-of-way (e.g., mileposts, curves, rail and highway grade crossings, switches, signals, track vertical profiles and horizontal geometry).

- Installing more than 28,500 custom-designed “wayside interface units” (WIU) that provide the mechanism for transmitting information from signal and switch locations along the right-of-way, to locomotives and railroad facilities.

- Integrating PTC technology on more than 17,200 Class I locomotives.

- Developing, producing, and deploying a new radio system specifically designed for the massive data transmission requirements of PTC at all base stations, trackside locations, and PTC-capable locomotives.

Significantly, PTC was developed with cyber threats in mind – which was not the case with older industrial control systems that have been targeted in cyber-attacks. A critical element of this effort entailed focused risk assessments of the design of PTC and its components and communications nodes and links – to identify and resolve potential concerns in development, prior to installation, and to narrow cyber risk when PTC was implemented through effective protective capabilities. Security measures were designed into the system in a layered, defense-in-depth approach that includes encryption, an array of security technologies, and redundant checks – which accords with federal cyber-security guidelines and international standards.

PTC can be viewed as a set of safety controls. Indeed, it is best viewed as simply an overlay to the safety critical control systems – and so does not affect the risk profile of the control systems. The local physical characteristics of the control system will continue to operate in a fail-safe condition.

Combined, freight railroads expect to spend more than $10 billion — their own funds, not taxpayer funds — on PTC development and deployment, by the time it is fully operational nationwide. Maintaining the PTC systems once they are installed, will cost hundreds of millions of additional dollars each year – again, railroads' funds, not taxpayer.

In the meantime, Class I railroads will continue to test and validate their systems thoroughly, to ensure they work as they should. Every day, as railroads finalize their PTC installation and expand PTC operations, additional accident avoidance becomes attainable.

IV. CYBER THREATS AND PREPAREDNESS

a. What are railroads experiencing?

Illicit cyber activity directed against the railroad industry has not targeted operational systems. Generally, railroads and industry organizations have experienced a range of activity that aligns with that directed against organizations in other critical infrastructure sectors. None of the activity has appeared to be overtly rail industry-specific.

The following types of cyber-activities have been experienced and reported by railroads and industry organizations in recent years:

- Spear-phishing emails
  - Most are not well-crafted
  - Most blocked by automated screening and protective measures
  - Key protective measure: sustained and effective user education in railroads cyber security programs

- Well-crafted phishing emails reported to government security and law enforcement agencies and shared for industry-wide awareness

- Attempts to commit fraud by misuse of corporate identity
  - Fake emails, purportedly from CEO, directing Vice President for Finance to wire transfer funds
  - Detection due to oddity of the requests, and anomalies in message format and content
  - Detected instances shared for industry-wide awareness and reported to government security and law enforcement agencies
  -

- Scans for information on corporate executives
  - Reviews of information online – on railroads' websites, professional networking sites, social media
  - Can be a preparatory step for attempts to conduct spear-phishing or attempt financial fraud
  - Detected activity shared for industry-wide awareness and reported to government security and law enforcement agencies
  -

- Occasional high volume, or otherwise suspect activity, from foreign internet protocol (IP) addresses
  - Source and technical indicators identified by affected railroad or industry organization
  - Detected activity shared for industry-wide awareness and reported to government security and law enforcement agencies
  -

- Compromises of email accounts of shippers or other industry entities
  - Generally, this activity has entailed purported dissemination of a document for review – with an embedded link that, if opened, expands the compromise/misuse
  - Quickly detected by network managers and users with other railroads and industry associations due to the odd or suspect nature of the emails and requested actions
  - Timely reporting has enabled dissemination of advisories that have blunted the effectiveness of these attempted email account compromises
  - Detected instances shared for industry-wide awareness and reported to government security and law enforcement agencies

- Falsified websites as cyber criminal activity intended to lure unsuspecting individuals to enter personal and financial information
  - Reporting by passenger railroads and public transportation agencies that maintain online sites for purchases of passenger tickets or fare cards
  - Domain names and site addresses align with common misspellings or added punctuation resulting from typographical errors made by individuals
  - Detected instances shared for industry-wide awareness and reported to government security and law enforcement agencies

- One confirmed targeted ransomware attempt

- Malicious software embedded in attached file in email
- Effectively detected and isolated by the receiving railroad
- Content of message, file type and designation, and other technical indicators shared for industry-wide awareness, and reported to government security and law enforcement agencies
- Some other detected and reported spearphishing attempts may have been part of an effort to perpetrate ransomware attacks
- No ransomware infections have impacted railroads operating in North America

b. Preparedness for Cybersecurity

Railroads have organized and prepared to meet the challenges of cyber threats and the potential of operations and business activity in a degraded information technology environment. The principal concern in railroads' cybersecurity programs is protection of systems involved in the management, monitoring, or control of train operations.

The railroad industry maintains a cyber-focused committee to foster cooperative efforts, sharing of cyber security information on threats, incidents, and related concerns, and pooling of effective practices – all for the purpose of narrowing overall risk profile.

The Rail Information Security Committee (RISC), together with the Rail Security Working Committee, which focused primarily on terrorism and other physical security concerns, forms the Rail Sector Coordinating Council (SCC). The Rail SCC meets the coordinating structure defined by the National Infrastructure Protection Plan (NIPP).

- Established in 1999, and continuously maintained since, the Rail Information Security Committee (RISC) is the focal point of the industry's unified, coordinated cybersecurity program and, among other things, acts as an industry forum for consultations among cyber security professionals to share information on threats and effective protective measures and risk mitigating actions.
- The RISC is comprised of the chief information security officers and cyber security leads for the Class I freight railroads (BNSF Railway, Canadian Pacific, CN, CSX Transportation, Kansas City Southern, Norfolk Southern, Union Pacific), Amtrak, Genesee and Wyoming Railroad, VIA Rail, and Railinc, supported by the Association of American Railroads (AAR) and the American Short Line and Regional Railroad Association (ASLRRA).
- RISC members maintain the requisite security clearances to enable sharing and discussion of classified material. This industry-initiated and sustained committee provides a consistent communication and coordination channel for effective interaction with government agencies and joint cyber security working groups.
- Both individually and through the RISC, railroads and industry organizations conduct comprehensive cyber risk assessments based on realistic threat scenarios drawn from intelligence analyses, including "penetration testing" that simulates an attack from malicious outsiders.
- The RISC facilitates evaluations of the security posture of railroads and industry organizations against the elements of the "Cybersecurity Framework," produced in a joint effort led by DHS and the National Institute of Standards and Technology

(NIST), in conjunction with the private sector, to meet a specific directive of Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, issued in February 2013, and subsequently endorsed by the current Administration by EO 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, issued in May 2017.

- Through the cooperative work in the Committee, railroads and industry organizations:
  - Maintain an industry Information Sharing and Analysis Center (ISAC) for collection, evaluation, and dissemination of cyber threat alerts and advisories, with recommended protection actions, drawn from diverse sources.
  - Define and periodically review and update specific intelligence requirements with government agencies and ministries in the United States and Canada, to ensure timely awareness, understanding, and action to address prevailing and emerging cyber threats.
  - Participate regularly in classified presentations and discussions on cyber threats and incidents with the Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), Transportation Security Administration (TSA), National Security Agency (NSA), Defense Security Service (DSS), Department of Transportation (DOT), Transport Canada, and the Royal Canadian Mounted Police (RCMP).
  - Engage directly with the National Cybersecurity and Communications Integration Center (NCCIC), the United States Computer Emergency Readiness Team (US-CERT), and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for continuous cyber threat awareness through timely sharing of information on threats and potential security concerns.
  - Share information on actual or suspected illicit cyber activity detected by network monitoring systems and firewalls – across the rail industry, with representatives of other modes of transportation and sector, and with government organizations.
  - A coordinated effort of the Rail Information Security Committee has produced a compilation of effective practices to guide procurements – across the industry, by freight and passenger railroads of all sizes – of information technology systems, networks, software, and supporting components.
  - Committee members have engaged with suppliers, to expand capabilities to assure mutual cyber threat awareness, and facilitate design and development for mitigation of cyber risk in new systems.

Further, railroads and industry organizations strive persistently to enhance their cybersecurity in a number of other ways, including:

- Maintaining cyber incident response plans that are tested regularly and enable preparedness to act effectively in case of a cyber-attack.
- Incorporating a variety of safeguards into their business and operational practices, such as tools to enhance capabilities for continued operations under adverse conditions and protocols that only allow authorized personnel access to key IT systems.
- Conducting regular comprehensive vulnerability assessments (including "penetration testing" that simulates an attack from malicious outsiders) and participating in recurring, coordinated industry- and government-sponsored cybersecurity exercises. • Hiring highly

skilled cybersecurity professionals who receive continual training to keep them abreast of current threats and best responses.

- Increasing the use of software and other emerging technologies to detect and quarantine cybersecurity threats.
- Hiring highly skilled cybersecurity professionals who receive continual training to keep them abreast of current threats and industry standards, policies, and regulations and new technologies and analytics.
- Users of computer networks in railroads receive recurring cyber security training, with drills employed to test awareness and understanding of appropriate actions to address potential threats and concerns – efforts that meet a fundamental objective defined in the NIST Framework and international standards.
- Railroads and industry organizations regularly exercise and enhance cyber security prevention and incident response plans, both internally and as an industry.
- The annual industry-wide exercise is conducted to assure clear understanding of actions to take to address cyber threats and incidents. It employs realistic scenarios, tests plans, and communications, as well as procedures for coordinated decision-making and for increases in alert level and security posture. Based on insights gained from risk assessments, cyber threat advisories, and experience gained in drills and exercises, railroads and industry organizations have incorporated a variety of effective safeguards and protective measures into business and operational practices.
- Finally, railroads and industry organizations maintain highly skilled cyber security experts who receive continual training to keep them abreast of current threats and effective responses.

c. Constant Need for Timely Information

The cyber threat landscape is constantly evolving. Protecting the rail network – its operations, infrastructure, networks and systems, and, most importantly, people – is a continuous effort. In this context, it is vital that the industry have access to timely and accurate cyber threat intelligence and related security information.

The worst-case scenario is the potential for missing opportunities to protect networks and systems, and to prevent breaches and intrusions, due to a lack of timely intelligence and related security information about an ongoing cyber-attack campaign or other developing threat of potential security or safety concern. For this reason, railroads set as a priority, continuous engagement, through the Rail Information Security Committee, with government security agencies, for attention to and action on, defined intelligence requirements, focused on cyber-attack tactics, as well as current and emerging threats and concerns, with information being shared at classified and unclassified levels.

- Involved government agencies include the Federal Bureau of Investigation (FBI); Department of Homeland Security (DHS), notably through its Cybersecurity and Infrastructure Security Agency (CISA), formerly the Office of Infrastructure Protection, and the National Cybersecurity and Communications Integration Center (NCCIC); the Transportation Security Administration (TSA); the Department of Transportation (DOT) and its modal agencies, the Federal Railroad Administration (FRA) and the

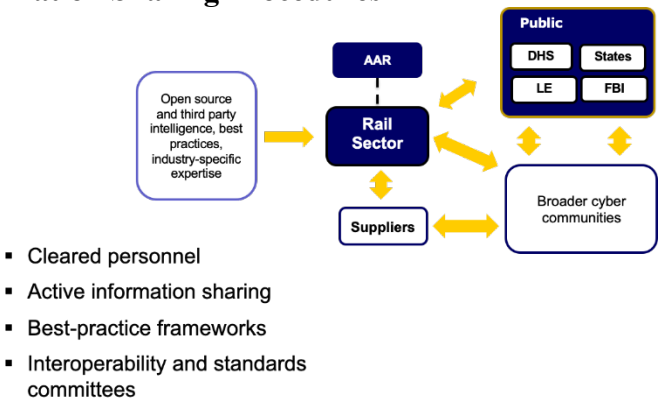
Pipeline and Hazardous Materials Safety Administration (PHMSA); the United States Coast Guard (USCG); and Transport Canada.

- Additionally, a dedicated industry alert network disseminates timely security information to the nation's freight and passenger railroads almost daily.
- Also, railroads and industry organizations maintain arrangements to receive cyber threat intelligence from reliable private sources.

Through this comprehensive effort, railroads continuously receive, evaluate, and share information on cyber threats, incidents, and security concerns on a daily basis – for the purpose of informing effective security practices, measures and procedures. Further, railroads and industry organizations strive to learn from cyber incidents and adverse impacts sustained in other modes of transportation and across other critical infrastructure sectors. This broad focus contributes to a better understanding of how illicit activities are planned and executed. The resulting insights are applied to refine protective measures and response plans, as warranted.

In summary, well-developed intelligence requirements and capabilities, and procedures for information analysis and sharing, ensure railroads' cyber security leads maintain continuous awareness of cyber-attack tactics, as well as current and emerging threats and concerns.

d. Intelligence Requirements and Information Sharing Procedures



In September, 2012, the Rail Information Security Committee initially presented its intelligence requirements to TSA, DHS, and the FBI. The requirements are regularly reviewed. Updates, as well as requests driven by reported developments or concerns in illicit cyber activity, have been submitted on multiple occasions since – to ensure the industry's priorities remain viable, we continue to ask for timely, relevant, and actionable intelligence and related security information on current and emerging threats.

To support continuously meeting the railroad industry's cybersecurity intelligence priorities, and help inform the industry's security measures and related preparedness actions, DHS, the FBI, and TSA have expanded their options for sharing and discussing classified information in a timely manner.

- Deployment of secure telephone equipment (STE) to major railroads and AAR, enabling direct consultations with federal government officials and among industry cyber security leads. Should federal authorities assess that the industry faces an elevated or imminent threat, this capability ensures timely sharing of classified intelligence and related security recommendations.

- To advance the strategic objective of harmonizing cross-border security awareness and preparedness, in an achievement unique in the critical infrastructure community, the railroad industry has attained approval of sharing of classified information from United States government sources, with cleared officials with CN (Canadian National), Canadian Pacific (CP), and, more recently, VIA Rail, Canada's national passenger railway, who hold clearances issued by the government of Canada. In reciprocation, Canadian authorities have hosted classified threat briefings for representatives of US-based railroads and industry organizations who hold Secret clearances issued by US government agencies.
- A classified information sharing network is established with TSA, enabling industry security and law enforcement leads with the requisite security clearance to access secure facilities maintained by the agency's Field Intelligence Officers (FIOs) in dozens of metropolitan areas nationally. Again, the beneficial result is, should elevated or imminent threat circumstances warrant, the industry's cleared law enforcement and security leads can enter any TSA FIO facility, obtain the needed briefing, review the relevant materials, and understand the nature of the concern – enabling timely risk-mitigating actions.
- A further expansion of the capability to share classified threat intelligence and to discuss security implications and protective actions and measures derives directly from a cross-sector initiative with DHS to establish a secure video teleconference (SVTC) network. More than 40 metropolitan areas in the United States have been linked simultaneously through this network, with representatives of each critical infrastructure sector and sub-sector participating. This capability is available for use to convene security coordinators, law enforcement officers, executives, and their designees, who hold appropriate security clearance (Secret or higher), within a sector or sub-sector. Venues offering access include state and local fusion centers, DHS/CISA field offices (staffed by Protective Security Advisors), some TSA secure facilities at airports, and a limited number of FBI field offices. Classified briefing and discussions focused on cyber threats, led by analysts with NSA, DHS, DOT, and the FBI, have been provided through this network.
- Bottom line: As a result of this collective effort, reflecting exceptional cooperation between government and industry, what had formerly taken weeks to months of effort – arranging in-person briefings or meetings in Washington, DC, or regional locations – can now be accomplished within a matter of hours.

Finally, two unique elements of the railroad industry's preparedness merit consideration. First, to assure thoroughness in access to classified and unclassified threat intelligence and related security information, the industry works closely with the FBI's National Joint Terrorism Task Force (NJTTF) Rail Security Program (RSP). The RSP includes Rail Liaison Agents (RLA), who are assigned to Joint Terrorism Task Forces (JTTF) and FBI Field Offices. RLAs maintain the ability to share intelligence and security-related information in their assigned areas, with law enforcement and security officials for freight and passenger railroads and mass transit agencies. A senior railroad police special agent is detailed at the RSP, as the industry's dedicated liaison to the FBI, on the full range of matters supportive of

preparedness for prevention of and response to acts of terrorism, serious crime, and disruptive cyber activity.

Second, in an innovative application of the public-private partnership, joint government-industry initiative links analysts from the FBI, TSA, Amtrak, the American Public Transportation Association (APTA), the Public and Surface Transportation Information Sharing and Analysis Center (PT/ST-ISACs), and the Association of American Railroads (AAR) in the Rail Intelligence Working Group (RIWG) for review of threat reporting, classified and unclassified, on potential security concerns and production of rail-focused intelligence analyses. This point is significant – government and industry analysts working together to develop products for dissemination to railroads, freight and passenger, in the United States and Canada. Disseminated widely among security and law enforcement professionals in industry and government, these materials provide accurate and timely intelligence, presented in a relevant and practically applicable context, with recommendations on actions relating to preparedness and security posture. Most importantly, they are a source of proven reliability to inform and guide risk assessments, training and awareness efforts with employees, and determination and implementation of effective and sustainable protective measures.

6. Government Support

Beyond continuous efforts to enhance the quality and dissemination procedures for cyber threat intelligence and related security information, classified and unclassified, federal government organizations, executive and legislative, should be guided by the following premises:

- Prescriptive regulatory actions should be avoided – because the measures they require are quickly outstripped by a constantly evolving, dynamic threat. Adherence to obsolete requirements stifles innovation. Instead, policymakers should rely on cooperative efforts through performance-based approaches that focus attention and effort on the outcome, not the method. A performance-based approach assures the flexibility and adaptability required to confront ever-changing cyber threats.
- Additional attention should be focused on cybersecurity vulnerabilities and the development and production of OT/IT hardware and software.
- Great care must be taken to ensure that commercially sensitive information on cyber incidents and cyber threats reported to the government is protected from inappropriate uses or public disclosure. The damage to organizational reputations and potential liability from misuse or careless handling of this sensitive information can be substantial and enduring.
- Existing federal entities with cybersecurity responsibilities should be streamlined – to meet the priority of assuring that useful intelligence and security information shared in a timely, effective, and consistent manner. Even the most effective cybersecurity plans and procedures will falter if useful information on cyber threats is not shared, which is why timely intelligence and information sharing is essential if cybersecurity efforts are to succeed. Specific emphasis should focus on sharing tactical intelligence on what perpetrators are doing and how they are doing it.

- Mandated certification requirements or standards for cybersecurity workers are unnecessary in the rail industry because railroads already use extensive background checks and other means to identify job applicants who might pose a security risk.