Committee on Transportation and Infrastructure
U.S. House of Representatives
Washington DC 20515

Peter A. DeFazio
Chair

Katherine W. Dedrick
Staff Director

Sam Graves
Ranking Member

Paul J. Sass
Republican Staff Director

November 1, 2021

SUMMARY OF SUBJECT MATTER

TO: Members, Committee on Transportation and Infrastructure
FROM: Staff, Committee on Transportation and Infrastructure
RE: Full Committee Hearing on "The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure"

PURPOSE

The Committee on Transportation and Infrastructure (T&I) will meet on Thursday, November 4, 2021, at 10:00 a.m. EDT in 2167 Rayburn House Office Building and via Zoom, to hold a hearing titled "The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure." The Committee will hear testimony from Scott Belcher on behalf of the Mineta Transportation Institute, Michael Stephens of the Tampa International Airport, Megan Samford of Schneider Electric, John Sullivan of the Boston Water and Sewer Commission on behalf of the Water Information Sharing and Analysis Center (WaterISAC), Gary Kessler of Gary Kessler Associates on behalf of The Atlantic Council, and Tom Farmer of the Association of American Railroads.

BACKGROUND

Cyberthreats to U.S. Infrastructure

Cyberattacks are a serious and evolving risk that affect transportation and infrastructure matters across T&I's jurisdiction. This hearing will focus on the needs of T&I stakeholders and the gaps in the nation's ability to prevent, prepare for, respond to, and recover from cyberattacks against infrastructure.

A common term that has sprung up for use within the government sector is "critical infrastructure," which according to Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, includes 16 sectors whose systems and networks, whether physical or virtual, "are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[1] T&I's jurisdiction includes five of these sectors, including Transportation Systems, Government Facilities, Water and Wastewater Systems, Dams, and Emergency Services.[2]

The nation's critical infrastructure is comprised of both public and private sector assets.[3] However, within T&I's jurisdiction, cybersecurity requirements in the private sector are mainly voluntary. Like other industries and the federal government, the transportation sector is facing a critical shortage of cybersecurity personnel, which has impacted the ability to protect, detect, and respond to cyberattacks effectively.[4] Simple steps regarding basic training, consistent cybersecurity hygiene, and periodic exercises could go a long way in protecting America's transportation infrastructure.[5] As the technology that enables America's infrastructure becomes ever more complex and increasingly integrated, cybersecurity threats and vulnerabilities will continue to multiply.

Impact of Cyberattacks

Cyberattacks can result in tremendous financial damage, destruction of infrastructure assets, and even death. They impact governments, businesses, and individuals alike and have been growing in number and sophistication. Late last year, it was discovered that a Russian-backed cyber campaign had installed malware in software updates that were received by as many as 18,000 customers of an American firm, SolarWinds, which develops software for businesses and governments.[6] The Department of Homeland Security (DHS) released an updated alert on the SolarWinds hack in April 2021, warning that DHS "determined that this threat poses a grave risk to the Federal Government and state, local, tribal, and territorial governments as well as critical infrastructure entities and other private sector organizations."[7]

Also, earlier this year, a ransomware attack on the Colonial Pipeline shut down the company's flow of fuel to the East Coast for nearly one week, causing fuel shortages and increasing fuel prices.[8] In April 2021, Chinese hackers reportedly penetrated New York City's Metropolitan

---

[1] The White House, *Presidential Policy Directive-Critical Infrastructure Security and Resilience,* (February 12, 2013), *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[2] U.S. House of Representatives Committee on Transportation and Infrastructure, *Committee Rules 2021–2022*, (Adopted February 4, 2021), *available at* https://www.govinfo.gov/content/pkg/CPRT-117HPRT43188/pdf/CPRT-117HPRT43188.pdf.

[3] Cybersecurity and Infrastructure Security Agency (CISA), *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience,* (2013), *available at* https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

[4] The Washington Post, *The Cybersecurity 202: The government's facing a severe shortage of cyber workers when it needs them the most*, (August 2, 2021), *available at* https://www.washingtonpost.com/politics/2021/08/02/cybersecurity-202-governments-facing-severe-shortage-cyber-workers-when-it-needs-them-most/.

[5] Endpoint, *What is Cyber Hygiene and Why Does it Matter?,* (August 5, 2021), *available at* https://endpoint.tanium.com/what-is-cyber-hygiene-and-why-does-it-matter/.

[6] Bloomberg, *SolarWinds Hack Leaves Critical Infrastructure in the Dark on Risks,* (January 5, 2021), *available at* https://www.bloomberg.com/news/newsletters/2021-01-05/solarwinds-hack-leaves-critical-infrastructure-in-the-dark-on-risks.

[7] CISA, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations,* (released December 17, 2020, revised April 15, 2021), *available at* https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

[8] Washington Post, *Panic buying strikes Southeastern United States as shuttered pipeline resumes operations,* (May 12, 2021), *available at* https://www.washingtonpost.com/business/2021/05/12/gas-shortage-colonial-pipeline-live-updates/.

Transit Agency, although no damage was reported.[9] In May 2021, the Washington Suburban Sanitary Commission, which provides water and wastewater service to 1.8 million people in two Maryland counties, was also the victim of a ransomware attack.[10]

Complex Jurisdictional Landscape

Cybersecurity efforts for the transportation sector are led jointly by the Department of Transportation (DOT), the Transportation Security Administration (TSA), and the U.S. Coast Guard.[11] In the water and wastewater sector, the Environmental Protection Agency (EPA) is designated as the lead agency, and its efforts are supported by the Cybersecurity and Infrastructure Security Agency (CISA).[12]

Increasing Vulnerabilities

Critical infrastructure sectors are facing more significant vulnerabilities for various reasons, including the proliferation of information technology and increasing digital access to computer networks.[13] Previously, critical infrastructure equipment was only accessible at its physical site.[14] To make any change to the system would require physically accessing the equipment.[15] Today, progress in technology, especially the Internet, has changed the risk landscape entirely with new and evolving ways to access systems which have made infrastructure assets more financially efficient and operationally effective while at the same time making them more vulnerable to cyber threats.[16] Demand for remote work, especially due to the COVID-19 pandemic, has dramatically increased vulnerabilities, with more employees needing remote access to systems.[17] However, making remote access to systems easier introduces significant vulnerabilities that bad actors can take advantage of to access those systems remotely.[18] Robust cybersecurity protocols can make remote access more secure. However, they can be time and work-intensive and not always possible depending on a facility's staffing and cybersecurity experience.[19] A vulnerability due to the use of a remote access

---

[9] NBC 4 NYC, *MTA Hacked in April Cyberattack; Employee, Customer Info Was Not Compromised,* (June 2, 2021), *available at* https://www.nbcnewyork.com/news/local/mta-hacked-in-april-cyberattack-employee-customer-info-was-not-compromised/3086785/.

[10] WSSC Water, *WSSC Water Investigating Ransomware Cyberattack*, (June 25, 2021), *available at* https://www.wsscwater.com/news/2021/june/wssc-water-investigating-ransomware-cyberattack.

[11] CISA, *Transportation Systems Sector*, (accessed on October 22, 2021), *available at* https://www.cisa.gov/transportation-systems-sector and CISA, *Water and Wastewater Systems Sector*, (accessed on October 22, 2021), *available at* https://www.cisa.gov/water-and-wastewater-systems-sector.

[12] The White House, *PPD-21 Critical Infrastructure Security and Resilience* (Feb 12, 2013), *available at* https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/.

[13] Government Accountability Office (GAO), *Technology Assessment: Cybersecurity for Critical Infrastructure Protection,* (May 28, 2004), *available at* https://www.gao.gov/products/gao-04-321.

[14] George Brown College, *The Evolution of PLCs*, (July 21, 2021), *available at* https://www.plctechnician.com/news-blog/evolution-plcs.

[15] *Id.*

[16] Coolfire Core, *What Is the Difference Between IT and OT?,* (April 12, 2019), *available at* https://www.coolfiresolutions.com/blog/difference-between-it-ot/.

[17] McKinsey, *Building cyber resilience in national critical infrastructure*; U.S. News and World Report, *Remote Working Fueled by COVID Pandemic Gaining Popularity,* (September 25, 2021), *available at* https://www.usnews.com/news/best-states/minnesota/articles/2021-09-25/remote-working-fueled-by-covid-pandemic-gaining-popularity.

[18] Securicon, *The Difference Between IT and OT, and How They Are Converging.*

[19] Verve, *Securing OT Systems: Is Remote Access Here to Stay?*, (April 18, 2020), *available at* https://verveindustrial.com/resources/blog/securing-ot-systems-is-remote-access-here-to-stay/.

program was how hackers were able to access a water treatment plant in Oldsmar, Florida earlier this year, for instance.[20]

The vulnerability of transportation infrastructure to cyberattacks will increase in the future as bad actors make greater use of emerging technologies, which create new vulnerabilities to exploit.[21] Cyberattacks that exploit an unknown vulnerability, known as a "zero-day" attack, provide no option or "zero days," to fix the issue before it is successfully used as part of a hack since the attack takes advantage of a new and previously unknown security flaw.[22] New technologies provide greater opportunities for zero-day attacks since they take advantage of technology that is new to cybersecurity professionals.[23] In addition, many emerging technologies in the transportation and infrastructure space will have various interconnected digital channels, providing multiple pathways for potential attackers.[24] Autonomous vehicles and unmanned aircraft systems are two key examples of emerging technologies that create multiple cybersecurity challenges for the future.[25]

High-Profile Cyberattacks Illustrate Range of Threats

Threats to infrastructure systems are increasing, as seen through several recent high-profile attacks against transportation infrastructure. Three such attacks include the recent ransomware attack on the Colonial Pipeline in May 2021,[26] the 2017 NotPetya malware attack that affected the Maersk shipping company,[27] and the February 2021 intrusion into the water treatment plant in Oldsmar, Florida.[28] Each of these attacks were distinct and highlighted the risks facing vital infrastructure entities, as well as opportunities for improving both government and private sector coordination and oversight of these vulnerabilities.

<u>Ransomware – Colonial Pipeline</u>

On May 7, 2021, Colonial Pipeline, one of the nation's largest oil and gas pipelines, was the victim of a ransomware attack by DarkSide, a cyber-criminal group believed to operate out of

---

[20] Mass.gov, *Cybersecurity Advisory for Public Water Suppliers*, (accessed on October 13, 2021), *available at* https://www.mass.gov/service-details/cybersecurity-advisory-for-public-water-suppliers.
[21] AT&T, *Emerging Technologies and the Cyber Threat Landscape,* (December 13, 2017), *available at* https://cybersecurity.att.com/blogs/security-essentials/emerging-technologies-and-the-cyber-threat-landscape
[22] FireEye, *What is a Zero-Day Exploit?* (accessed on October 20, 2021), *available at* https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html.
[23] *Id.*
[24] Boston Consulting Group, *Navigating Rising Cyber Risks in Transportation and Logistics,* (August 30, 2021), *available at* https://www.bcg.com/publications/2021/navigating-rising-cyber-risks-in-transportation-and-logistics
[25] ScienceDaily, *Need to safeguard drones and robotic cars against cyber attacks*, (November 27, 2019), *available at* https://www.sciencedaily.com/releases/2019/11/191127121302.htm
[26] Matt Egan and Clare Duffy, CNN, *Colonial Pipeline launches restart after six-day shutdown*, (May 12, 2021), *available at* https://www.cnn.com/2021/05/12/business/colonial-pipeline-restart/index.html.
[27] Jordan Novet, CNBC, *Shipping company Maersk says June cyberattack could cost it up to $300 million* (August 16, 2017) *available at* https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html.
[28] Colonial Pipeline, *Media Statement Update: Colonial Pipeline System Disruption*, (May 17, 2021), *available at* https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption; Wired, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, (Aug 22, 2018), *available at* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/; Pinellas County Sheriff Department YouTube channel, *Treatment Plant Intrusion Press Conference*, (February 8, 2021), *available at* https://www.youtube.com/watch?v=MkXDSOgLQ6M&t=1s.

Russia.[29] The attack was discovered when an employee found a digital ransom note on a system in the Colonial information technology (IT) network.[30] DarkSide encrypted all of Colonial's IT systems and demanded a financial payment in exchange for a key to unlock the impacted systems.[31] Though the attack did not directly affect Colonial's operational technology (OT)[32] network, which is used to control the pipeline equipment, company officials immediately halted operations throughout the pipeline. They did so to isolate and contain the damage and ensure the malware did not spread to the OT network.[33] The following day, Colonial made a $4.4 million ransom payment to DarkSide and received the information it needed to regain control of its IT systems.[34] Colonial began work immediately to restore pipeline operations with the assistance of the Pipeline and Hazardous Materials Safety Administration (PHMSA) at DOT, which provided guidance on temporary manual operations of the pipeline and its subsequent return to service.[35] On May 13, 2021, six days after the attack, it had fully restored service, though several more days passed before the fuel supply chain returned to normal.[36]

An investigation conducted by cybersecurity consulting firm FireEye-Mandiant (Mandiant) determined that the attackers used an employee's legacy username and password to log in to a virtual private network (VPN) device.[37] Several missteps helped enable DarkSide to access Colonial's network in this manner.[38] First, the employee's login information was no longer in use, but had not been deleted from the company's system.[39] Second, the legacy VPN profile did not require multi-factor authentication, such as the use of a one-time passcode, which CISA and the Federal Bureau

---

[29] Hearing before the House Committee on Homeland Security, *Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure,* (June 9, 2021), *available at* https://www.govinfo.gov/content/pkg/CHRG-117hhrg45085/pdf/CHRG-117hhrg45085.pdf; Federal Bureau of Investigation, *FBI Deputy Director Paul M. Abbate's Remarks at Press Conference Regarding the Ransomware Attack on Colonial Pipeline*, (June 7, 2021), *available at* https://www.fbi.gov/news/pressrel/press-releases/fbi-deputy-director-paul-m-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline.

[30] House Committee on Homeland Security, *Cyber Threats in the Pipeline.*

[31] *Id.*

[32] Operational technology (OT) is equipment that handles machines and their physical operation. OT includes hardware and software that interacts with the physical environment, including monitoring and controlling industrial equipment, assets, processes, and events. Historically, IT and OT networks were entirely isolated from one another since they developed separately, with OT predating IT. OT used relatively simple systems that completed specific functions that were only accessible on-site and in-person. This provided physical isolation for OT networks, and when IT and the Internet were developed, that isolation prevented OT from being accessed remotely. This segmentation was good for security. However, there were business demands for remote visibility into industrial operations, leading businesses to move towards a more integrated system. An integrated system has productivity benefits, including reducing administrative burdens, streamlining work, and improving data to inform better decision-making. Unfortunately, it also creates and greatly expands a network's cyber vulnerabilities. A connection to an IT network can serve as a path to access OT networks. The safest version of an OT network is one that is completely separated and has no external connectivity with IT networks or the Internet, known as an air gap. An air gap is a security measure where a system is not connected to any other network or device and can only be accessed physically.

[33] House Committee on Homeland Security, *Cyber Threats in the Pipeline.*

[34] *Id.*

[35] U.S. DOT, PHMSA, *Remarks of Acting Administrator Tristan Brown at API's Midstream Committee Meeting,* (May 26, 2021), *available at* https://www.phmsa.dot.gov/news/remarks-tristan-brown-before-api-midstream-committee.

[36] Colonial Pipeline, *Media Statement Update: Colonial Pipeline System Disruption*, (May 17, 2021), *available at* https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption.

[37] House Committee on Homeland Security, *Cyber Threats in the Pipeline.*

[38] *Id.*

[39] *Id.*

of Investigation (FBI) recommend as a best practice.[40] Third, the employee had used the same password on a different website, from which the password had been stolen.[41] CISA recommends using unique passwords for each device or account.[42] The president and CEO of Colonial has said that his company has disabled the legacy VPN account, has instituted multi-factor authentication for network access, and is taking other steps to strengthen its cyber defenses.[43]

Colonial's pipelines transport nearly half of the East Coast's fuel, providing energy for more than 50 million Americans. The impact of the ransomware attack was felt throughout the eastern United States.[44] The shutdown resulted in massive fuel shortages and gasoline panic-buying.[45] At least 12,000 gas stations in 11 states reported being completely empty, and the price of gas surpassed $3 a gallon.[46] The day before Colonial fully resumed operations, 65 percent of gas stations in North Carolina reported being out of gas; in Georgia, South Carolina, and Virginia, more than 43 percent of gas stations reported being out of gas.[47] The governors of Florida, North Carolina, and Virginia all declared states of emergency to help alleviate the fuel shortages.[48]

The Colonial attack illustrated how intrusions into pipeline computer networks have the potential to negatively affect the nation's security, economy, and well-being.[49] The perpetrators of the attack also accessed personally identifiable information, such as names, birth dates, and Social Security numbers for more than 5,800 current and former Colonial employees, exposing these individuals to the risk of fraud and identity theft.[50]

In response to the attack, TSA—which oversees pipeline security[51]—issued security directives that require, among other things, pipeline owners and operators to take measures to protect against cyberattacks to their IT and OT systems and to develop and implement a

---

[40] *Id*; CISA, *Alert (AA21-131A): DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks*, (May 11, 2021), *available at* https://us-cert.cisa.gov/ncas/alerts/aa21-131a and FBI, *OPS Cyber Awareness Guide*, (accessed on October 22, 2021), *available at* https://www.fbi.gov/file-repository/cyber-awareness-508.pdf/view.
[41] House Committee on Homeland Security, *Cyber Threats in the Pipeline.*
[42] CISA, *Security Tip (ST04-003): Good Security Habits*, (February 21, 2021), *available at* https://www.cisa.gov/tips/st04-003.
[43] Hearing before the Senate Committee on Homeland Security and Governmental Affairs, *Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack, Testimony of Joseph Blount, President and Chief Executive Officer of the Colonial Pipeline Company*, (June 8, 2021), *available at* http://www.hsgac.senate.gov/download/testimony-blount-2021-06-08.
[44] See: Senate Committee on Homeland Security and Governmental Affairs, *Testimony of Joseph Blount* and House Committee on Homeland Security, *Cyber Threats in the Pipeline.*
[45] Washington Post, *New emergency cyber regulations lay out 'urgently needed' rules for pipelines but draw mixed reviews*, (October 3, 2021), available at https://www.washingtonpost.com/national-security/cybersecurity-energy-pipelines-ransomware/2021/10/03/6df9cab2-2157-11ec-8200-5e3fd4c49f5e_story.html.
[46] Washington Post, *Panic buying strikes Southeastern United States.*
[47] *Id.*
[48] New York Times, *Gas Pipeline Hack Leads to Panic Buying in the Southeast*, (May 11, 2021), *available at* https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html.
[49] TSA, *Written Testimony of David P. Pekoske, Administrator, Transportation Security Administration, U.S. Department of Homeland Security*, Hearing Pipeline Security, Before the Committee on Commerce, Science, and Transportation," (July 27, 2021), *available at* https://www.commerce.senate.gov/services/files/3DFD1053-A11E-4B1A-9818-FE29C19AA06B.
[50] ZD Net, *Colonial Pipeline sends breach letters.*
[51] TSA also coordinates with PHMSA on pipeline security under a Memorandum of Understanding, *See: PHMSA, Annex to the Memorandum of Understanding Between the Department of Homeland Security and the Department of Transportation Concerning Transportation Security Administration and Pipeline and Hazardous Materials Safety Administration Cooperation on Pipeline Transportation Security and Safety*, Feb. 26, 2020, *available at :* https://www.phmsa.dot.gov/sites/phmsa.dot.gov/files/docs/regulatory-compliance/phmsa-guidance/73466/phmsa-tsa-mou-annexexecuted.pdf.

cybersecurity contingency and recovery plan.[52] Although the Colonial attack was carried out on the company's IT network, it highlights the highly interconnected nature of OT operations that businesses must consider.[53] Experts say that actions like applying security patches and updates promptly and using multi-factor authentication can help protect against ransomware and other cyberattacks.[54]

Malware – NotPetya & Maersk Shipping

In 2017 Russian linked individuals reportedly unleashed a malware attack in Ukraine named NotPetya.[55] The malware affected virtually every federal agency in the country, crippling four hospitals in the capital, six power companies, two airports, more than 22 Ukrainian banks, as well as freezing ATMs and card payment systems in retail and transit sectors.[56] Ukraine later estimated that NotPetya wiped 10 percent of all computers in the country, and one government official said immediately after the attack, "the government was dead."[57]

Within hours, NotPetya had propagated far beyond Ukraine, affecting computer networks in companies in 65 countries around the world.[58] Among the companies affected were the multinational shipping company Maersk ($300 million in damage), the pharmaceutical giant Merck ($800 million), the French construction company Saint-Gobain ($384 million), FedEx's European subsidiary ($400 million), as well as smaller victims such as a hospital in Pennsylvania and a chocolate company in Australia.[59] The White House would later identify NotPetya as the most destructive and costly cyberattack in history, with overall damage above $10 billion.[60] The malware even infected the Russian state oil company, Rosneft, demonstrating the runaway nature of NotPetya's harms.[61] The U.S. issued sanctions against organizations involved in NotPetya's release and, in 2020, the Department of Justice indicted six Russian military officers for the cyberattack.[62]

---

52 *Id.*

53 Dragos, *Recommendations Following the Colonial Pipeline Cyber Attack*, (May 11, 2021), *available at* https://www.dragos.com/blog/industry-news/recommendations-following-the-colonial-pipeline-cyber-attack/.

54 ZD Net, *Ransomware is the biggest cyber threat to business. But most firms still aren't ready for it*, (October 11, 2021), *available at* https://www.zdnet.com/article/ransomware-is-now-the-most-urgent-cyber-threat-to-business-but-most-firms-arent-ready-for-it/.

55 Wired, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, (Aug 22, 2018), *available at* https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

56 *Id*,

57 *Id.*

58 Jai Vijayan, *3 Years After NotPetya, Many Organizations Still in Danger of Similar Attacks,* Dark Reading, (June 30, 2020), *available at* https://www.darkreading.com/threat-intelligence/3-years-after-notpetya-many-organizations-still-in-danger-of-similar-attacks.

59 Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History,* (October 14, 2018), *available at* https://tech.industry-best-practice.com/2018/10/14/the-untold-story-of-notpetya-the-most-devastating-cyberattack-in-history/.

60 *Id.*; The White House, *Statement from the Press Secretary*, (Feb 15, 2018), *available at* https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

61 Wired, *Petya Ransomware Hides State-Sponsored Attacks, Say Ukrainian Analysts,* (June 28, 2017), available at https://www.wired.com/story/petya-ransomware-ukraine/.

62 U.S. Dept of Justice, *Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, (Oct 19, 2020), *available at* https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

Maersk is the world's largest container shipping company, responsible for shipping an estimated 25 percent of the world's food supply.[63] It is a $56 billion company present in 130 nations with over 700 ships and 17 percent of the world's cargo shipping container capacity.[64] The malware entered Maersk's IT network through a computer in the Ukrainian port of Odessa.[65] There, a finance executive had earlier asked IT administrators to upload the Ukrainian accounting program on a single computer.[66] From that computer, NotPetya propagated through the Maersk global IT system in seven minutes.[67] Within an hour, all Maersk's end-user devices, including 49,000 laptops and printers and 3,500 of 6,200 servers, were effectively destroyed.[68] Maersk's fixed phoneline ceased functioning and, due to system integration, all Outlook and cell phone contacts were wiped, crippling initial response efforts.[69] Though ships' computers were not affected, the software at Maersk terminals which received files from their ships, informing terminal operators of ships' content and how to direct cargo handling, had been wiped.[70] Paralysis resulted at seventeen Maersk terminals worldwide for days, with no one able to receive cargo for ground transport and perishable and time-sensitive materials stuck in place.[71]

Rebuilding Maersk's network began four days after the attack when the company recovered its domain controller, a detailed map of their network that controlled system users, from a Maersk office in Ghana where a coincidental power outage had protected the office's IT system.[72] A Maersk official flew with a copy of the critical software to England, where over five days, hundreds of IT workers used the recovered domain controller to reconstruct Maersk's active directory for worldwide operations, build out 2,000 new laptops, and reenable core business processes and systems.[73] It took several more days before Maersk could restart online shipment processes and more than a week before terminals around the world could function normally.[74] Over two months passed before Maersk IT personnel fully restored its software setup.[75]

Following the NotPetya attack, Maersk leadership shared their critical takeaways with the global community, which assisted many other NotPetya victims in recovery.[76] These included

[63] Statista, *The world's leading container ship operators as of September 30, 2021, based on number of owned and chartered ships*, (accessed on October 22, 2021), *available at* https://www.statista.com/statistics/197643/total-number-of-ships-of-worldwide-leading-container-ship-operators-in-2011/.
[64] Statista, *Number of APM-Maersk ships from February 2021 to September 2021,* (September 30, 2021), *available at* https://www.statista.com/statistics/199366/number-of-ships-of-apm-maersk-in-december-2011/; Statista, *Moeller-Maersk's assets from FY 2018 to FY 2020,* (February 24, 2021), *available at* https://www.statista.com/statistics/325993/total-assets-of-moeller-maersk/; Maersk, *A.P. Moller – Maersk enters strategic partnership with Danish Crown on global end-to-end logistics,* (October 15, 2021), *available at* https://www.maersk.com/news/articles/2021/10/15/maersk-enters-strategic-partnership-with-danish-crown.
[65] Wired, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.*
[66] *Id.*
[67] Andy Powell, *Implementing the Lessons Learned from a Major Cyberattack*, (November 2019), *available at* https://www.youtube.com/watch?v=wQ8HIjkEe9o.
[68] Rae Richie, *Maersk: Springing back from a catastrophic cyberattack*, Aug 2019), *available at* https://www.i-cio.com/management/insight/item/maersk-springing-back-from-a-catastrophic-cyber-attack.
[69] *Id.*
[70] Wired, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.*
[71] *Id.*
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] Wired, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.*
[76] Andy Powell, *Implementing the Lessons Learned from a Major Cyberattack*; *see also* Jim Snabe, *CyberSecurity Davos 2017 – Maersk*, (June 2017), *available at* https://www.youtube.com/watch?v=VaqIYlYmDbA.

transparency, open communication, crisis recovery and business continuity plans, regular cyber incident response exercises, and a network of consultancies and government actors, among others.[77]

Intrusions – Oldsmar Wastewater Treatment Plant

On Friday, February 5, 2021, a hacker remotely accessed the computer system of the water treatment plant for the city of Oldsmar, Florida, which provides water to about 15,000 people.[78] The hacker changed chemical levels in the water, increasing the sodium hydroxide (otherwise known as lye) level from 100 parts per million to 11,100 parts per million.[79] In small quantities, sodium hydroxide is used to control acidity in water, but at higher levels, it is dangerous to humans. If the affected water had made it to the city's residents, they could have become seriously ill.[80] Ingesting as little as 10 grams of sodium hydroxide can be fatal.[81]

The hack at Oldsmar was discovered immediately when an employee noticed programs being opened on his computer and that the level of sodium hydroxide in the water had changed.[82] The employee first noticed his computer being accessed remotely earlier that day but had not reported it because it was common for supervisors or others to access the system to troubleshoot issues remotely.[83] Upon noticing later that the system was being remotely accessed again and that chemical levels were being changed to dangerous levels, the employee changed the chemical levels back to a safe level and reported the intrusion.[84] The plant disabled remote access to their system after the hack and reported the hack to federal authorities.[85]

CISA and the FBI determined that the hackers gained access to the supervisory control and data acquisition (SCADA) system, likely exploiting cybersecurity weaknesses such as poor password security and an outdated operating system.[86] They also determined that hackers were likely able to access the SCADA system through the remote access TeamViewer software, which used the same password across all computers and lacked any firewall protection.[87] City officials have said that

---

77 *Id.*
78 Pinellas County Sheriff Department YouTube channel, *Treatment Plant Intrusion Press Conference*, (February 8, 2021), *available at* https://www.youtube.com/watch?v=MkXDSOgLQ6M&t=1s and Tampa Bay Times, *Someone tried to poison Oldsmar's water supply during hack, sheriff says*, (February 8, 2021), *available at* https://www.tampabay.com/news/pinellas/2021/02/08/someone-tried-to-poison-oldsmars-water-supply-during-hack-sheriff-says/.
79 Pinellas County Sheriff Department YouTube channel, *Treatment Plant Intrusion Press Conference.*
80 The New York Times, *Dangerous Stuff: Hackers Tried to Poison Water Supply of Florida Town*, (February 8, 2021), *available at* https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html.
81 Environmental Protection Agency (EPA), *Sodium Hydroxide*, (September 1992), *available at* https://www3.epa.gov/pesticides/chem_search/reg_actions/reregistration/fs_PC-075603_1-Sep-92.pdf.
82 Pinellas County Sheriff Department YouTube channel, *Treatment Plant Intrusion Press Conference.*
83 Reuters, *Hackers try to contaminate Florida town's water supply through computer breach,* (February 8, 2021), *available at* https://www.reuters.com/article/us-usa-cyber-florida-idUSKBN2A82FV.
84 Pinellas County Sheriff Department YouTube channel, *Treatment Plant Intrusion Press Conference.*
85 Vice, *Hacker Tried to Poison Florida City's Water Supply*, Police Say, (February 8, 2021), *available at* https://www.vice.com/en/article/88ab33/hacker-poison-florida-water-pinellas-county.
86 CISA, *Alert (AA21-042A) Compromise of U.S. Water Treatment Facility*, (February 12, 2021), *available at* https://us-cert.cisa.gov/ncas/alerts/aa21-042a.
87 ABC Action News WFTS Tampa Bay, *FBI: Water system hack likely caused by remote access program, old software and poor password security*, (February 10, 2021), *available at* https://www.abcactionnews.com/news/local-news/i-team-

residents were never at risk because of the city's automated monitoring of the water's pH levels and its built-in alarms, which would have been triggered before the water made it to the public.[88]

The Oldsmar hack provides an example of the vulnerability of water systems to cybersecurity threats, especially smaller systems that lack the security controls, IT staff, and funding of larger organizations. It also shows how remote management applications, though efficient, create opportunities for attacks.[89] The water sector is well-protected from a large-scale attack on the entire system due to its decentralized nature, but the existence of thousands of small utilities across the country makes it challenging to ensure compliance with best practices throughout the entire sector.[90] The investigations from CISA, the FBI, and others, for example, show that the Oldsmar water treatment plant had poor password management, an outdated operating system, and an old remote access management system still on computers.[91] Further, an analysis done by Nozomi Networks' Labs determined that the Oldsmar hack was not very sophisticated and that it was likely perpetrated by someone without specific background knowledge of the water treatment process.[92]

Poor Cybersecurity Hygiene Creates Weak Links

As reliance on IT continues to dominate American lives and global competitiveness, the Colonial, Maersk, and Oldsmar attacks illustrate the cybersecurity vulnerabilities found in common items and the willingness of enemies, whether nation-state or not, to target these gaps. Cybersecurity in both the public and private sector can be significantly enhanced by making easy fixes, such as ensuring known software patches are implemented quickly, providing regular cybersecurity awareness training to staff, and using effective passwords and other authentication systems.[93] However, the federal government, organizations, and individuals often fail to take these "cyber hygiene" measures due to resource constraints or lack of awareness or will, creating easy targets for cybercriminals. These weak links may result in consequences that threaten the nation's transportation infrastructure and networks and potentially harm the public.

Recent surveys of the public transit and water and wastewater utilities sectors confirm that some U.S. transportation infrastructure assets are not making some of the recommended adjustments.[94] These surveys show gaps in the water and transit sectors' ability to detect, confront,

---

investigates/fbi-water-system-hack-likely-caused-by-remote-access-program-old-software-and-poor-password-security; Mass.gov, *Cybersecurity Advisory for Public Water Suppliers*, (accessed on October 4, 2021), *available at* https://www.mass.gov/service-details/cybersecurity-advisory-for-public-water-suppliers and FBI, CISA, EPA, MS-ISAC, *Joint Cybersecurity Advisory*, (February 11, 2021), *available at* https://www.mass.gov/doc/joint-fbi-cisa-cybersecurity-advisory-on-compromise-of-water-treatment-facility/download.

88 Pinellas County Sheriff Department YouTube channel, *Treatment Plant Intrusion Press Conference.*

89 FBI, CISA, EPA, MS-ISAC, *Joint Cybersecurity Advisory.*

90 CISA, *Water and Wastewater Systems Sector*, (accessed on October 27, 2021), *available at* https://www.cisa.gov/water-and-wastewater-systems-sector.

91 FBI, CISA, EPA, MS-ISAC, *Joint Cybersecurity Advisory.*

92 Nozomi Networks, *Hard Lessons From the Oldsmar Water Facility Cyberattack Hack*, (February 10. 2021), *available at* https://www.nozominetworks.com/blog/hard-lessons-from-the-oldsmar-water-facility-cyberattack-hack/.

93 Cybersecurity & Infrastructure Security Agency (CISA), *Cyber Essentials Starter Kit: The Basics for Building a Culture of Cyber Readiness,* (Spring 2021), *available at* https://www.cisa.gov/sites/default/files/publications/Cyber%20Essentials%20Starter%20Kit_03.12.2021_508_0.pdf

94 Water Sector Coordinating Council, *Water and Wastewater Systems – Cybersecurity: 2021 State of the Sector,* (June 2021), *available at* https://www.waterisac.org/system/files/articles/FINAL_2021_WaterSectorCoordinatingCouncil_Cybersecurity_State_

and respond to cybersecurity incidents.[95] Research into other relevant T&I industries, such as aviation and maritime, indicates similar security vulnerabilities.[96]

- **Water Sector Survey.** In June 2021, water security stakeholders issued a report that included a survey of more than 600 water and wastewater utilities regarding cybersecurity gaps and needs.[97] More than 57 percent of water utilities that responded to the survey have a risk management plan that addresses cybersecurity threats, while 42 percent do not.[98] Further, 26 percent conduct cybersecurity risk assessments less than once per year.[99] More than 37 percent of small water utilities said they don't share cybersecurity data because they don't know who to share this information with or how to do so, while 22 percent feared the data would not be kept confidential.[100] While 75 percent of respondents have implemented or are in the process of implementing some "cyber protection efforts," more than 25 percent of water utilities have no plans to conduct these efforts. Nearly 64 percent do not employ a chief information security officer (CISO), and while over 50 percent of water utilities conduct some cybersecurity-related drill or exercises, 42 percent do not.[101] More than 68 percent do not participate in any cybersecurity-related drills or exercises, but 47 percent said they need cybersecurity technical assistance, advice, and other support, and 41 percent said they need federal grants or loans to improve cybersecurity.[102]

- **Transit Sector Survey.** The Mineta Transportation Institute and San Jose State University produced a recent report on transit-related cybersecurity issues that included a survey of 90 transit agencies serving more than 124 million people.[103] Among the results, over 50 percent of those surveyed had up to four staff dedicated to cybersecurity while nearly 39 percent had no dedicated staff, three of which are considered "extra-large" agencies with more than $100 million in operating expenses.[104] In addition, four of 20 agencies that reported having a cybersecurity incident still have no staff dedicated to cybersecurity.[105] Over 60 percent of transit agencies surveyed provide cybersecurity training to staff, while more than 24 percent provide no training, and more than 58 percent of those that don't provide training said it was due to a lack of resources.[106] In addition, 42 percent of the agencies don't have an

---

of_the_Industry-17-JUN-2021.pdf and Scott Belcher, et. al., *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*, San Jose State University and Mineta Transportation Institute, (September 2020), *available at* https://transweb.sjsu.edu/sites/default/files/1939-Belcher-Transit-Industry-Cyber-Preparedness.pdf.

[95] *Id.*

[96] *See, e.g.*, For Aviation Cybersecurity, Airways Magazine, *The Current State of Cybersecurity in Civil Aviation* (June 5, 2021), *available at* https://airwaysmag.com/industry/the-current-state-of-cybersecurity-in-civil-aviation and for Maritime Cybersecurity, Atlantic Council, *Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity* (Oct. 2021), pp 5-13, *available at* https://www.atlanticcouncil.org/wp-content/uploads/2021/10/Cyber-Maritime-Final-Report.pdf.

[97] Water Sector Coordinating Council, *Water and Wastewater Systems – Cybersecurity: 2021 State of the Sector.*

[98] *Id.*

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] Scott Belcher, et. al., *Is the Transit Industry Prepared for the Cyber Revolution? Policy Recommendations to Enhance Surface Transit Cyber Preparedness*, San Jose State University and Mineta Transportation Institute, (September 2020), *available at* https://transweb.sjsu.edu/sites/default/files/1939-Belcher-Transit-Industry-Cyber-Preparedness.pdf.

[104] *Id.*

[105] *Id.*

[106] *Id.*

incident response plan, and of those that had one, over half have not had an exercise in over a year.[107] Nearly 78 percent of the 90 agencies surveyed said they had not had a cybersecurity "incident."[108] The authors found this troubling since given the frequency of cyberattacks, it suggests that many of these transit agencies may simply not be detecting successful cybersecurity penetrations against their networks.[109] In addition, more than 30 percent of those that said they had been the victim of a cybersecurity incident also said they never reported the incident to anyone.[110]

Private-Public Coordination

In the United States, it is generally cited that 85 percent of critical infrastructure is in private hands, and much of the transportation sector is subject to some government oversight.[111] As such, cooperation between the public and private sectors that fosters integrated, collaborative engagement and interaction is essential to maintaining transportation infrastructure cybersecurity, especially as technology makes transportation infrastructure increasingly vulnerable to cyberattacks.[112] The annual cost of malicious cyber activity to the U.S. economy, estimated recently at between $57 billion and $109 billion, demonstrates the pressing need for action in both the private and public sectors.[113]

As the federal government seeks to strengthen transportation infrastructure's cyber defenses, with an emphasis on cybersecurity preparedness, the perspective and experience of the private sector remains vital to create effective cyber resilience.[114] Addressing the biggest gaps, including those discussed below, will require collaboration between public and private stakeholders.

Cybersecurity Workforce Shortages

There is a dire shortage globally of workers with cybersecurity expertise. In the U.S., recent estimates show around 950,000 individuals currently employed in this field, with a need to fill an additional 464,000 cyber-related positions.[115] In the public sector alone, there are about 60,000 individuals employed in cyber jobs, with an additional 36,000 unfilled positions across all levels of government.[116]

In addition, a Center for Strategic and International Studies survey of public and private sector organizations in eight countries, including the United States, found that eighty-two percent of

---

[107] *Id.*
[108] *Id.*
[109] *Id.* at 36-37.
[110] *Id.*
[111] Lawfare, *Is It Really 85 Percent?* (May 11, 2021), *available at* https://www.lawfareblog.com/it-really-85-percent.
[112] CISA, *Critical Infrastructure Sector Partnerships*, (accessed on Oct 22, 2021) *available at* https://www.cisa.gov/critical-infrastructure-sector-partnerships.
[113] Council of Economic Advisors, *The Cost of Malicious Cyber Activity to the U.S. Economy* (2018), *available at* https://trumpwhitehouse.archives.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/
[114] Lawfare, *Is It Really 85 Percent?*
[115] CyberSeek, "Cybersecurity Supply/Demand Heat Map," *last accessed on October 22, 2021, at* https://www.cyberseek.org/heatmap.html; Washington Post, *The Cybersecurity 202: The government's facing a severe shortage of cyber workers when it needs them the most*, (August 2, 2021), *available at* https://www.washingtonpost.com/politics/2021/08/02/cybersecurity-202-governments-facing-severe-shortage-cyber-workers-when-it-needs-them-most/.
[116] *Id.*

responding organizations have a shortage of employees with cybersecurity skills.[117] The survey results also show that the shortage of cybersecurity professionals can have real consequences. One-third of respondents said a shortage of skills makes their organizations more desirable hacking targets, and a quarter said insufficient cybersecurity staff strength has damaged their organization's reputation and led directly to the loss of proprietary data through a cyberattack.[118]

Although a shortage of federal cybersecurity workers remains, the federal government has taken several steps to address this shortage.[119]

- The Office of Management and Budget directed the Office of Personnel Management and other federal agencies to establish programs to assist federal agencies in using existing compensation flexibilities and explore opportunities for new or revised pay programs for cybersecurity positions to better enable them to compete with other employers.[120]
- CISA created the National Initiative for Cybersecurity Education framework for increasing the size and capability of the U.S. cyber workforce, and Girls Who Code, an effort to develop pathways for young women to pursue careers in cybersecurity and technology.[121]
- The United States Digital Service allows technology specialists to apply and essentially take a "tour of civic service" to bring real-world private sector knowledge into the federal government.[122]

Voluntary Standards and New Federal Leadership

In 2013, in response to an Executive Order, the National Institute of Standards and Technology (NIST) began developing the first national cybersecurity framework consistent with its mission to promote U.S. innovation and competitiveness.[123] In May 2017, applying the framework, widely touted by cybersecurity experts, became mandatory for federal agencies.[124] Compliance is still

---

[117] Center for Strategic and International Studies, *Hacking the Skills Shortage: A study of the international shortage in cybersecurity skills*, (July 2016), *available at* https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf.
[118] *Id.*
[119] Washington Post, *The Cybersecurity 202*.
[120] Office of Management and Budget, "Memorandum for Heads of Executive Departments and Agencies: Federal Cybersecurity Workforce Strategy," (July 12, 2016), *available at* https://www.chcoc.gov/content/federal-cybersecurity-workforce-strategy.
[121] CISA, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, (accessed on October 22, 2021)*, at* https://www.cisa.gov/nice-cybersecurity-workforce-framework and CISA, *Girls Who Code Announce Partnership to Create Career Pathways for Young Women in Cybersecurity and Technology*, accessed on October 22, 2021, *available at* https://www.cisa.gov/news/2021/09/30/cisa-and-girls-who-code-announce-partnership-create-career-pathways-young-women.
[122] U.S. Digital Service, "Our Mission," *accessed on* https://www.usds.gov/mission.
[123] NIST, *History and Creation of the Framework*, (accessed on October 22, 2021), *available at* https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework.
[124] NIST, *Questions and Answers*, (accessed on October 22, 2021), *available at* https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics; Brandon Vigliarolo, *NIST Cyber Security Framework: A Cheat Sheet for Professionals* (March 5, 2021), *available at* https://www.techrepublic.com/article/nist-cybersecurity-framework-the-smart-persons-guide/.

voluntary in the private sector, with NIST estimating a 50 percent adoption rate among private actors in 2020.[125]

In May 2021, President Biden issued Executive Order (EO) 14028 focused on improving the nation's cybersecurity and protecting federal government networks, building on past executive action, including executive orders issued in 2017 and 2013.[126] Although the primary aim of the EO is to strengthen federal systems, it also notes that much of the nation's infrastructure is owned and operated by the private sector and encourages these companies to "follow the Federal government's lead and take ambitious measures to augment and align cybersecurity investments with the goal of minimizing future incidents."[127] The EO also establishes a Cybersecurity Review Board, modeled after the National Transportation Safety Board, composed of private sector entities and federal officials to review significant cyberattacks and share lessons learned.[128]

Following the EO, in June 2021, CISA issued guidance on Ransomware for Operators of Critical Infrastructure.[129] CISA's guidance addresses increasingly complex IT and OT systems that play a pivotal role in critical infrastructure, where the attack surfaces have expanded well beyond once-isolated systems.[130] The guidance will assist in establishing standards for preparing, mitigating, and responding to cyberattacks targeting critical infrastructure.[131]

In July 2021, the Biden administration also issued the National Security Memorandum on *Improving Cybersecurity for Critical Infrastructure Control Systems*.[132] The memorandum called for creating cyber-performance goals for critical infrastructure companies, including the establishment of baseline cybersecurity performance standards across all infrastructure sectors.[133]

The Biden administration has supplemented voluntary cooperative efforts with new mandatory standards to protect critical infrastructure in some sectors.[134] At the end of July, TSA issued a security directive requiring owners and operators of TSA-designated critical pipelines to

---

[125] NIST, *Cybersecurity Framework*, *available at* https://www.nist.gov/industry-impacts/cybersecurity-framework/ (*last visited October 22, 2021*).
[126] The White House, *Executive Order on Improving the Nation's Cybersecurity*, (May 12, 2021), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/; *see also* The White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, (May 11, 2017), available at https://www.govinfo.gov/content/pkg/DCPD-201700327/pdf/DCPD-201700327.pdf; The White House, *Improving Critical Infrastructure Cybersecurity*, (Feb. 12, 2013), *available at* https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636.
[127] The White House, *FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cyber Security and Protect Federal Government Networks*, (May 12, 2021), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/.
[128] *Id.*
[129] CISA, *Rising Ransomware Threat to Operational Technology Assets* (June 9, 2021).
[130] CISA, *FACT SHEET: Rising Operational Threat to Operating Technology Assets*, *available at* https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf (*last visited* October 22, 2021).
[131] *Id.*
[132] The White House, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*, (July 28, 2021), *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.
[133] *Id.*, Sec. 4.
[134] CRS, *Pipeline Cybersecurity: Federal Programs*, (September 9, 2021), pp 9-11, *available at* https://crsreports.congress.gov/product/pdf/R/R46903.

implement specific mitigation measures to protect against ransomware attacks and other known threats to IT and OT systems, develop and implement a cybersecurity contingency and recovery plan, and conduct a cybersecurity architecture design review to supplement mandatory cyber protocol requirements related to pipelines issued two months earlier.[135] TSA is reportedly preparing similar directives for the rail and aviation sectors. The DHS Secretary reports the administration continues "coordinating and consulting with industry as we develop all of these plans."[136] Given the Committee's role in the safety of transportation industries, as TSA issues directives, it will closely monitor these directives.

Voluntary Reporting and Lack of Government Data Sharing

Reporting cybersecurity incidents—across the critical infrastructure spectrum—is also largely voluntary, a decades-old legacy of the days before large-scale cyberattacks and networked critical infrastructure.[137] Many actors responsible for critical infrastructure agree that what should be reported and to whom in the federal, state, and local governments regarding a cyber incident can be unclear.[138] Further, requiring private entities to report cybersecurity-related data to the government has long been subject to debate, and the complexity of some proposed reporting models has raised concerns about the disproportionate burdens placed on smaller private actors.[139] Therefore, a complete understanding of the cyber threats to the nation is likely underestimated in the face of these dynamics. In 2016, for example, the FBI estimated that only 15 percent of cybercrime victims reported the crime to law enforcement.[140]

Recent EO 14028 also encourages sharing cyber-related threat data between the private sector and the federal government and requires federal IT contractors to report cyber incidents to the government, although reporting cyber incidents from privately-owned infrastructure assets or transportation systems remains voluntary.[141] Obtaining a more holistic picture of the cyber threats our transportation systems and infrastructure assets face may help improve their own responses and the federal government's ability to identify these threats.[142]

---

135 *Id.*, p 10.
136 DHS, *Secretary Mayorkas Delivers Remarks at the 12th Annual Billington CyberSecurity Summit* ,(October 6, 2021), *available at* https://www.dhs.gov/news/2021/10/06/secretary-mayorkas-delivers-remarks-12th-annual-billington-cybersecurity-summit.
137 Tatiana Tropina, *Public–Private Collaboration: Cybercrime, Cybersecurity and National Security*, (May 7, 2015); Alan Raul and Vivek Mohan, *The Privacy, Data Protection and Cybersecurity Law Review – United States* (Sept. 2018), 276-403, *available at* https://datamatters.sidley.com/wp-content/uploads/2018/11/United-States.pdf.
138 Sujit Ramen, Bloomberg Law, *It's Time for National Cyber-Incident Reporting Legislation*, (July 12, 2021), *available at* https://news.bloomberglaw.com/us-law-week/its-time-for-national-cyber-incident-reporting-legislation.
139 Coalfire, *Compliance in the Era of Digital Transformation* (May 24, 2021); Alan Raul and Vivek Mohan, *The Privacy, Data Protection and Cybersecurity Law Review – United States* (Sept. 2018), 276-403, *available at* https://datamatters.sidley.com/wp-content/uploads/2018/11/United-States.pdf.
140 FBI, *2016 Internet Crime Report*, p. 4, (accessed on October 22, 2021), *available at* https://www.ic3.gov/Media/PDF/AnnualReport/2016_IC3Report.pdf.
141 The White House, *Executive Order on Improving the Nation's Cybersecurity*, (May 12, 2021). Sec. 2, *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.
142 CISA, *Information Sharing and Cyberawareness*, *available at* https://www.cisa.gov/information-sharing-and-awareness (*last visited* October 22, 2021).

While CISA leadership has recently expressed an interest in mandatory 24-hour reporting, potentially supported by fines for non-compliance, the private sector does not appear fully in favor of this approach.[143] Some private actors responsible for critical infrastructure have concerns with reporting cyber incidents to the federal government.[144] These concerns include bad press, regulatory reprisal, or minimal public consequences for cyber attackers.[145] Further, private actors who proactively seek out information from the federal government on current threats or reported vulnerabilities report being frustrated by the information sharing practices of the federal government.[146] Collaboration and coordination between the public and private sector in protecting the nation's critical infrastructure is critical, but still a work in progress.[147]

Conclusion

As America seeks to remain globally competitive and provide Americans with safe and secure infrastructure, cybersecurity will remain a top priority. During this hearing, the Committee will hear from private sector witnesses, but it intends to hold a second cybersecurity hearing on these issues in the future that will focus on federal agencies and their efforts to close the current cybersecurity gaps that put industry and government at greater risk of attacks, actions to assist the private sector, and what steps they are taking to implement recent federal cybersecurity directives.

---

143 Adam Mazmanian, FCW, *CISA Seeks 24-Hour Timeline for Cyber Incident Reporting* (Oct 19, 2021), *available at* https://fcw.com/articles/2021/10/19/cisa-wales-reporting-timeline-cyber-incident.aspx.

144 Amitai Etzioni, *The Private Sector: A Reluctant Partner in Cyber Security* (Dec 14, 2014), *available at* https://icps.gwu.edu/private-sector-reluctant-partner-cybersecurity.

145 Dan Swinhoe, CSO, *Why businesses don't report cybercrimes to law enforcement* (May 30, 2019), *available at* https://www.csoonline.com/article/3398700/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html.

146 Samantha Swartz, Cybersecurity Dive, *What Happens if Threat Data Isn't Shared?* (April 30, 2021), *available at* https://www.cybersecuritydive.com/news/information-sharing-threat-intelligence-analysis-cybersecurity/599319/; Jonathan Day and Michael Mahoney, *Private Sector Wants More-and Better-Cybersecurity Cooperation with Government* (Mar 9, 2020), *available at* https://morningconsult.com/opinions/private-sector-wants-more-and-better-cybersecurity-cooperation-with-government/.

147 Jason Miller, Federal News Network, (*CISA's still overcoming challenges 5 years after Cybersecurity Information Sharing Act became law,* October 6, 2020), *available at* https://federalnewsnetwork.com/reporters-notebook-jason-miller/2020/10/cisas-still-overcoming-challenges-5-years-after-cybersecurity-information-sharing-act-became-law/.

WITNESS LIST

Scott Belcher
President and Chief Executive Officer, SFB Consulting, LLC
Testifying on behalf of Mineta Transportation Institute

Megan Samford
Vice President and Chief Product Security Officer
Schneider Electric

Thomas L. Farmer
Assistant Vice President, Security
Association of American Railroads

Michael Stephens
General Counsel and Executive Vice President
Tampa International Airport

John Sullivan
Chief Engineer, Boston Water and Sewer Commission
Testifying on behalf of the Water Information Sharing and Analysis Center (WaterISAC)

Gary Kessler, PhD
President, Gary Kessler Associates
Testifying on behalf of The Atlantic Council