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 29, 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: Federal Perspectives on Securing the Nation's Infrastructure"

PURPOSE

The Committee on Transportation and Infrastructure will meet on Thursday, December 2, 2021, at 10:00 a.m. EST in 2167 Rayburn House Office Building and via Zoom, to hold a hearing titled "The Evolving Cybersecurity Landscape: Federal Perspectives on Securing the Nation's Infrastructure." The Committee will hear testimony from Mr. Cordell Schachter, Chief Information Officer (CIO), Department of Transportation (DOT); Mr. Larry Grossman, Chief Information Security Officer (CISO), Federal Aviation Administration (FAA); Ms. Victoria Newhouse, Deputy Assistant Administrator for Policy, Plans, and Engagement, Transportation Security Administration (TSA); Rear Admiral John W. Mauger, Assistant Commandant for Prevention Policy, U.S. Coast Guard (USCG); Mr. Kevin Dorsey, Assistant Inspector General for Information Technology Audits, DOT Office of Inspector General (DOT OIG); and Mr. Nick Marinos, Director of Information Technology and Cybersecurity, Government Accountability Office (GAO).

BACKGROUND

Cyberthreats to the U.S. Transportation and Infrastructure Sectors

Cyberattacks are a serious and evolving risk that affect transportation and infrastructure matters across T&I's jurisdiction. Cyberattacks can result in tremendous financial damage, destruction of infrastructure assets, and even death.[1] They impact governments, businesses, and individuals alike and have been growing in number and sophistication.[2] This hearing is the second of

[1] Council of Economic Advisors, "The Cost of Malicious Cyber Activity to the U.S. Economy," (February 2018), available at https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf; 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/

[2] Id.

two full committee hearings on cybersecurity of the nation's infrastructure.[3] The first hearing was held in November 2021 and featured testimony from industry stakeholders and cybersecurity experts.[4] As discussed in the November hearing, cyberattacks on the nation's critical infrastructure—about 85 percent of which is owned and operated by private entities[5]—can cause significant harm to the public. However, many private entities, as well as federal agencies, have not taken the necessary steps to prevent, prepare for, respond to, and recover from cyberattacks.[6] During the Committee's November hearing, witnesses discussed challenges that hamper infrastructure operators' preparedness and resilience, such as a shortage of qualified information technology staff, a lack of appropriate cybersecurity awareness training, and insufficient technical expertise.[7] Responsibility for cybersecurity of the nation's infrastructure is shared among many entities, including the federal government, state and local entities, and public and private infrastructure owners and operators.[8]

This hearing will feature federal witnesses and focus on (1) actions the federal government is taking to address cybersecurity and preparedness of the transportation and infrastructure sectors, and (2) challenges agencies face in securing their own computer networks and the steps they are taking to address these challenges and to implement recent federal cybersecurity directives and other actions.

Federal Agencies with a Role in Transportation and Infrastructure Cybersecurity

In 2013, the federal government established a framework to guide the cybersecurity efforts of critical infrastructure owners and operators, which is set forth in the *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*.[9] The plan organizes critical infrastructure into 16 sectors and designates a federal department or agency as the lead coordinator—or sector risk management agency—for each sector.[10]

---

[3] House Committee on Transportation and Infrastructure, "The Evolving Cybersecurity Landscape: Federal Perspectives on Securing the Nation's Infrastructure,"(December 2, 2021), available at https://transportation.house.gov/committee-activity/hearings/the-evolving-cybersecurity-landscape-federal-perspectives-on-securing-the-nations-infrastructure; House Committee on Transportation and Infrastructure, "Hearing: The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure," available at https://transportation.house.gov/committee-activity/hearings/the-evolving-cybersecurity-landscape-industry-perspectives-on-securing-the-nations-infrastructure

[4] Id.

[5] GAO, "The Department of Homeland Security's (DHS) Critical Infrastructure Protection Cost-Benefit Report," (June 26, 2009), p. 1, available at https://www.gao.gov/assets/gao-09-654r.pdf

[6] See for example, testimony of Scott Belcher and John Sullivan at House Committee on Transportation and Infrastructure, "Hearing: The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure," available at https://transportation.house.gov/committee-activity/hearings/the-evolving-cybersecurity-landscape-industry-perspectives-on-securing-the-nations-infrastructure

[7] "Hearing: The Evolving Cybersecurity Landscape: Industry Perspectives on Securing the Nation's Infrastructure," available at https://transportation.house.gov/committee-activity/hearings/the-evolving-cybersecurity-landscape-industry-perspectives-on-securing-the-nations-infrastructure

[8] The White House, PPD-21 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

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

[10] NIPP, 2013 at p. 9.

The agencies listed below serve as the federal interface for the prioritization and coordination of sector-specific security and resilience efforts, including for cybersecurity. These respective sectors are within the committee's jurisdictional purview.

Sector	Sector Risk Management Agencies
Government Facilities	General Services Administration Federal Protective Service (DHS)[11]
Transportation Systems	Department of Transportation U.S. Coast Guard (DHS) Transportation Security Administration (DHS)[12]
Water and Wastewater Services	Environmental Protection Agency[13]
Dams	Department of Homeland Security (DHS)[14]
Emergency Services	Department of Homeland Security (DHS)[15]

The responsibilities of sector risk management agencies include:[16]

- Coordination with the Department of Homeland Security (DHS) and other relevant departments and agencies, and collaboration with infrastructure entities on the protection of critical infrastructure, including cybersecurity threats;
- Providing and facilitating technical assistance for sector owners and operators to identify threats and vulnerabilities, improve cyber defenses, and help mitigate cyber incidents; and
- Participation in Sector-Specific Coordinating Councils, Government Coordinating Councils, and other coordinating bodies for their sector.[17]

Information Sharing and Analysis Centers

In addition to the above-mentioned federal assistance for cybersecurity, private industry offers assistance through sector-specific Information Sharing and Analysis Centers (ISAC). The concept of ISACs was first promulgated in Presidential Decision Directive-63 (PDD-63), signed on May 22, 1998.[18] Today the National Council of ISACs recognizes 26 industry specific ISAC organizations.[19] Typically, ISACs are nonprofit organizations that share information about threats,

[11] Department of Homeland Security and General Services Administration, "Government Facilities Sector-Specific Plan," 2015, available at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-government-facilities-2015-508.pdf
[12] Department of Homeland Security and Department of Transportation, "Transportation Systems Sector-Specific Plan," 2015, available at https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf
[13] NIPP, 2013 at p. 11.
[14] Id.
[15] Id.
[16] Id. at pp. 9-10.
[17] Id. at p. 43.
[18] "About ISACs," National Council of ISACs, available at https://www.nationalisacs.org/about-isacs
[19] "About NCI," National Council of ISACs, available at https://www.nationalisacs.org/about-nci

vulnerabilities, and mitigation within their particular sector.[20] Some also provide awareness training and assistance in responding to cyber and other security incidents.[21]

For example, in the water sector, the Water Information Sharing and Analysis Center (WaterISAC) partners with various organizations, including the American Water Works Association, the Association of Metropolitan Water Agencies, and the National Rural Water Association.[22] WaterISAC also maintains close contact with government agencies to access sensitive and classified security information.[23] WaterISAC acts as an information clearinghouse and provides analysis and resources to its members to "support response, mitigation, and resilience initiatives."[24]

Federal Cybersecurity Preparedness and Internal Weaknesses

While the federal government supports private actors regarding cybersecurity in critical infrastructure, significant work is needed within federal government agencies to improve their own cybersecurity defenses. In March 2021, GAO identified ten critical actions needed to address major cybersecurity challenges.[25] The ten urgent needs fell under four major cybersecurity challenges previously identified by GAO, specifically: (1) Establishing a comprehensive cybersecurity strategy and performing effective oversight; (2) Securing federal systems and information; (3) Protecting cyber critical infrastructure; and (4) Protecting privacy and sensitive data.[26]

The report also noted that establishing the Office of the National Cyber Director within the Executive Office of the President, as Congress did in early 2021, was "an essential step forward" towards addressing cybersecurity.[27] Further, the recently passed *Infrastructure Investment and Jobs Act* directed $21 million for initial funding for this office, ensuring the federal government will be better situated to confront the nation's cyber threats and challenges.[28]

However, the GAO report also said, "critical risks remain on supply chains, workforce management, and emerging technologies" and pointed out that in December 2020, "GAO reported that none of the 23 agencies in its review had fully implemented key foundational practices for managing information and communications technology supply chains."[29] In May 2021, GAO received updates from six of the 23 agencies regarding actions taken or planned to address its recommendations.[30] However, none of the agencies had fully implemented the recommendations.[31]

---

[20] National Council of ISACs web site, available at https://www.nationalisacs.org/about-isacs
[21] For example, Aviation ISAC offers training and incident response analysis see: https://www.a-isac.com/aboutus; Maritime Transportation System ISAC offers training and threat alerts see: https://www.mtsisac.org/services
[22] Water ISAC web site, available at https://www.waterisac.org/about-us
[23] Id.
[24] Id.
[25] GAO, "Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges," (March 2021), p. 9, available at https://www.gao.gov/assets/gao-21-288.pdf
[26] Id. at p. 8.
[27] Id. at p. i.
[28] Liz Carey, "Infrastructure Act Includes $20M for Office of National Cyber Director," Homeland Preparedness News, (November 9, 2021), available at https://homelandprepnews.com/stories/74682-infrastructure-act-includes-20m-for-office-of-national-cyber-director/
[29] GAO, "Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges," (March 2021), p ii, available at https://www.gao.gov/assets/gao-21-288.pdf
[27] GAO, "Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risk," (May 25, 2021), p 15, available at https://www.gao.gov/assets/gao-21-594t.pdf
[31] Id. at p. 13.

The report also highlighted the fact that since 2010, "GAO has made nearly 80 recommendations to enhance infrastructure cybersecurity" and that "nearly 50" of those recommendations have not been implemented heightening the risk to the nation's infrastructure.[32] Overall, since 2010, GAO has issued more than 3,700 recommendations across the federal government, including DOT and its subagencies, that could improve the nation's cybersecurity.[33] In July 2021, more than 950 of those recommendations remained unimplemented.[34]

Department of Transportation (DOT)

DOT and its 11 operating administrations and other components rely on hundreds of information technology systems for uses as diverse as air traffic control operations, disbursement of billions of dollars in loans and grants, managing sensitive personnel data, and many other functions key to DOT's mission.[35] The DOT OIG has identified information security as a top management challenge for the Department and stated that addressing these weaknesses and strengthening controls is essential for protecting departmental information technology (IT) infrastructure and improving DOT's cybersecurity posture.[36] These recurring cybersecurity weaknesses have resulted in key systems being vulnerable to cyberattacks, takeovers, and data breaches.[37] In addition, in the DOT OIG's most recent Top Management Challenges report released in late October 2021, they found that DOT needs a "holistic approach with sustained focus and direction" to resolve 66 open recommendations the DOT OIG made in previous audits.[38] These recommendations are intended to help address 10,663 security weaknesses identified in DOT plans of actions and milestones.[39] The DOT OIG has also identified cybersecurity weaknesses at the component agencies within DOT. Specific problems the DOT OIG has identified include the following:

- Federal Transit Administration (FTA). In October 2021, the DOT OIG released a report on cybersecurity weaknesses of FTA's financial management systems that could affect FTA's ability to approve, process, and disburse COVID-19 funds.[40] Among the OIG's findings: FTA has failed to fix security control weaknesses identified since 2016; it lacks sufficient contingency planning and incident response capabilities; and it "does not adequately monitor the security controls provided by or inherited from DOT's common control provider."[41] The DOT OIG found that 139 of 269 security controls were not

[32] GAO, "Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges," March 2021, p ii, available at https://www.gao.gov/assets/gao-21-288.pdf
[33] GAO, "Our Testimony to Congress on Efforts to Secure Oil and Gas Pipelines Against Cyberattacks," (July 28, 2021), available at https://www.gao.gov/blog/our-testimony-congress-efforts-secure-oil-and-gas-pipelines-against-cyberattacks-video
[34] Id.
[35] DOT OIG, "DOT Top Management Challenges FY 2022," (October 27, 2021), available at https://www.oig.dot.gov/sites/default/files/DOT%20FY%202022%20Top%20Management%20Challenges.pdf
[36] Id.
[37] Id.
[38] Id.
[39] Id.
[40] DOT OIG, "FTA Does Not Effectively Assess Security Controls or Remediate Cybersecurity Weaknesses To Ensure the Proper Safeguards Are in Place To Protect Its Financial Management Systems," (October 20, 2021), available at https://www.oig.dot.gov/sites/default/files/FTA%20Financial%20Management%20Systems%20Security%20Controls%20Final%20Report_10-20-21_REDACTED.pdf
[41] Id.

tested or implemented but reported as satisfied by FTA officials, for instance, increasing the exposure of FTA's financial management systems to outside threats.[42] The DOT OIG made 13 recommendations to correct these and other weaknesses and FTA has concurred with all of these recommendations.[43]

- Federal Motor Carrier Safety Administration (FMCSA). FMCSA regulates and oversees the safety of commercial vehicles. In October 2021, the DOT OIG issued a report showing their investigators had exploited vulnerabilities in web servers at FMCSA that allowed them to gain unauthorized access to the agency's network.[44] The agency also failed to detect the DOT OIG's placement of malware on their network.[45] DOT OIG investigators were able to gain access to 13.6 million unencrypted records with personally identifiable information.[46] The DOT OIG estimated that if malicious actors had obtained this information, it could have cost FMCSA up to $570 million in credit monitoring fees.[47] FMCSA did not detect the breach, in part because it did not use required automated detection tools and malicious code protections.[48] The DOT OIG also found that FMCSA does not always remediate vulnerabilities as quickly as DOT policy requires, putting FMCSA's network and data at risk for unauthorized access and compromise.[49] FMCSA concurred with DOT OIG's 13 recommendations and considers these issues "resolved but open pending FMCSA's completion of" its planned actions.[50]

- Federal Aviation Administration (FAA). In August 2021, the DOT OIG released a report on FAA's efforts to categorize its high-impact information systems.[51] The report found that until recently, the agency's air traffic organization had never properly categorized its high-impact security systems, although these systems provide safety-critical services.[52] In addition, it found, "FAA lacks formalized policies and procedures for selecting and implementing high security controls for its high-impact systems and continues to develop mitigations for security risks."[53] The DOT OIG further found that FAA has not completed a required gap analysis to comply with federal standards for its 45 high-impact systems "and is essential for determining whether the organization's security and privacy risks have been effectively managed."[54] Finally, the report said, "FAA has not yet mitigated the risk that the NAS [National Airspace System] could be

[42] Id.
[43] Id.
[44] DOT OIG, "FMCSA's IT Infrastructure Is at Risk for Compromise," (October 20, 2021), available at https://www.oig.dot.gov/sites/default/files/FMCSA%20IT%20Infrastructure%20Final%20Report_10-20-21%20REDACTED.pdf
[45] Id.
[46] Id.
[47] Id.
[48] Id.
[49] Id.
[50] Id.
[51] DOT OIG, "FAA Is Taking Steps to Properly Categorize High-Impact Information Systems but Security Risks Remain Until High Security Controls Are Implemented," (August 2, 2021), available at https://www.oig.dot.gov/sites/default/files/REDACTED%20Final%20Report%20on%20FAA%20System%20Security%20Re-Categorizations.pdf
[52] Id.
[53] Id.
[54] Id.

vulnerable to threats as the Agency works to implement high security controls, because it has not fully implemented enterprise security initiatives designed to protect NAS assets."[55]

- Aviation Cyber Initiative (ACI). ACI is an interagency collaboration between FAA, the Department of Homeland Security (DHS), and the Department of Defense (DOD) that was informally established in 2016.[56] Its objectives include identifying and analyzing cyber threats and vulnerabilities, engaging with aviation stakeholders to help reduce cyber risks, and seeking opportunities to improve risk mitigation.[57] Its charter was finally approved in 2019, when 10 priorities were set for 2019 and 2020. The DOT OIG found, however, that ACI has only implemented three of those priorities.[58] In addition, according to GAO, the FAA has not developed mechanisms to monitor and evaluate cybersecurity issues that are raised in ACI coordination meetings and FAA's "oversight coordination activities are not supported by dedicated resources within" the FAA's budget.[59] GAO declared in a report it released in October 2020: "Until FAA establishes a tracking mechanism for cybersecurity issues, it may be unable to ensure that all issues are appropriately addressed and resolved. Further, until it conducts an avionics cybersecurity risk assessment, it will not be able to effectively prioritize and dedicate resources to ensure that avionics cybersecurity risks are addressed in its oversight program."[60] In addition, GAO found more broadly that "FAA has not (1) assessed its oversight program to determine the priority of avionics cybersecurity risks, (2) developed an avionics cybersecurity training program, (3) issued guidance for independent cybersecurity testing, or (4) included periodic testing as part of its monitoring process."[61]

United States Coast Guard (Coast Guard or Service)

The aging and underinvested status of the Coast Guard's cyber systems and IT infrastructure is at a crisis point as was highlighted during a Subcommittee on Coast Guard and Maritime Transportation hearing on November 16, 2021.[62] The Coast Guard has historically struggled with IT

---

[55] Id.
[56] DOT OIG, "FAA and Its Partner Agencies Have Begun Work on the Aviation Cyber Initiative and Are Implementing Priorities," (September 2, 2020), p. 1, available at https://www.oig.dot.gov/sites/default/files/FAA%20Aviation%20Cyber%20Initiative%20Final%20Report%5E09-02-20.pdf
[57] DOT Office of Inspector General, "FAA and Its Partner Agencies Have Begun Work on the Aviation Cyber Initiative and Are Implementing Priorities," (September 2, 2020), p. 1, available at https://www.oig.dot.gov/sites/default/files/FAA%20Aviation%20Cyber%20Initiative%20Final%20Report%5E09-02-20.pdf; See also FAA, "Aviation Cyber Initiative (ACI)" available at https://www.faa.gov/air_traffic/technology/cas/aci/media/documents/aci.pdf
[58] Id.
[59] GAO, "AVIATION CYBERSECURITY: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks," GAO-21-86, (October 2020), available at https://www.gao.gov/products/gao-21-86
[60] Id.
[61] Id.
[62] House Committee on Transportation and Infrastructure, "Hearing: Rebuilding Coast Guard Infrastructure to Sustain and Enhance Mission Capability," (November 16, 2021), available at https://transportation.house.gov/committee-activity/hearings/rebuilding-coast-guard-infrastructure-to-sustain-and-enhance-mission-capability; James Ousman Cheek, "Changing Tides: Appraising and Supporting the Coast Guard's Role In Changing Seas," Consortium for Ocean Leadership, (November 2021), available at https://oceanleadership.org/changing-tides-appraising-and-supporting-the-coast-guards-role-in-changing-seas/

modernization, and Commandant Karl Shultz has made it a priority in what the Coast Guard calls its "Tech Revolution."[63] The Tech Revolution road map outlines strategic goals, including modernizing cybersecurity and cyber resilience.[64] Currently, the Coast Guard primarily operates on 1990s-era hardware and software, running the risk of critical failures even before its resilience can be challenged by cyber incidents.[65] In February 2020, for instance, the Commandant stated that the Coast Guard's IT infrastructure was at the "brink of catastrophic failure" and highlighted the immediate need for $300 million in IT spending to modernize the Coast Guard's technological landscape.[66]

In its 2015 *Cyber Strategy*, the Coast Guard explained that in the digital age, their overall mission to ensure the safety, security, and stewardship of the nation's waters cannot effectively be met without the Coast Guard maintaining a robust and comprehensive cyber program.[67] In 2021, working in close collaboration with DHS, DOD, government partners, foreign allies, and the maritime industry, the Coast Guard released its *Cyber Strategic Outlook*, an update to its cyber strategy to improve protection of the Marine Transportation System (MTS).[68] The strategic outlook focused on three efforts: (1) Securing resilient information technology and operational technology networks to support all Coast Guard missions; (2) Employing frameworks, standards, and best practices in prevention and response activities to identify and manage cyber risks to the MTS; and (3) Projecting advanced cyberspace capabilities in and through the operating environment enabling the Service to fight and win across all domains.[69]

The MTS includes waterways, shorelines, ports, shipyards, facilities, bridges, and other infrastructure throughout the United States, facilitating $5.4 trillion of economic activity every year, representing about a quarter of U.S. gross domestic product.[70] Over the past year, high-profile cyberattacks into U.S. networks have included crippling attacks on maritime infrastructure like the one that hit the Port of Kennewick, Washington, in November 2020.[71] The port refused to pay a $200,000 ransom to cybercriminals who hijacked their computer systems cutting off emails and other IT systems.[72] Email systems were restored by the end of the month, but it took longer to restore other compromised computer systems.[73]

---

[63] Lauren Williams, "As the Coast Guard wrestles with aging IT, cloud is a long-term conversation," FCW (August 2018), available at https://fcw.com/articles/2018/08/03/uscg-it-progress-williams.aspx

[64] United States Coast Guard, "Tech Revolution: Vision for the Future," available at https://www.dcms.uscg.mil/Portals/10/CG-6/roadmap/C5i-roadmap-FINAL-v6.pdf

[65] Connie Lee, "BREAKING: Coast Guard Releases New 'Tech Revolution' Road Map," National Defense, (February 2020), available at https://www.nationaldefensemagazine.org/articles/2020/2/20/coast-guard-releases-new-tech-revolution-roadmap

[66] Jackson Barnett, "Coast Guard wants a 'tech revolution' to dig itself out of IT from the '90s," Fed Scoop (February 2020), available at https://www.fedscoop.com/coast-guard-tech-revolution-plan/.

[67] Coast Guard, "United States Coast Guard Cyber Security Strategy" (June 2015), p. 10, available at https://www.dco.uscg.mil/Portals/10/Cyber/Docs/CG_Cyber_Strategy.pdf?ver=nejX4g9gQdBG29cX1HwFdA%3d%3d

[68] Coast Guard, "United States Coast Guard Cyber Strategic Outlook," (August 2021), p. 4, available at https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf

[69] Id. at p. 7.

[70] Id. at p. 3.

[71] Tri-City Areas Journal of Business, "Cyberattack Hobbles Port of Kennewick," (December 2020), available at https://www.tricitiesbusinessnews.com/2020/12/port-cyberattack/

[72] Id.

[73] Id.

As the sector risk management agency responsible for protecting the MTS under DHS's designated critical infrastructure sectors, the Coast Guard designated its Captains of Port to "lead governance by promoting cyber risk management, accountability, and the development and implementation of unified response plans."[74] The Coast Guard also intends to "refine cybersecurity incident reporting requirements and promote information sharing to improve the ability of owners and operators to prepare for, mitigate, and respond to threats to maritime critical infrastructure."[75]

Under the 2021 *Cyber Strategic Outlook,* the Coast Guard intends to conduct offensive cyber operations to deny or degrade adversaries' ability to plan, fund, communicate, or execute their own cyber operations.[76] To enable that capability, the Coast Guard seeks to establish an offensive Cyber Mission Team, interoperable with DOD cyber forces and DHS, and requested funding for continued cyber force development as part of its fiscal year (FY) 2022 budget request.[77] Supplementing a Coast Guard Maritime Cyber Readiness Branch that already consists of three defensive Cyber Protection Teams, administrative and policy legal challenges remain for the Coast Guard's future cyber operations capability.[78]

Federal Emergency Management Agency (FEMA)

In February 2021, DHS modified two existing FEMA Preparedness Grant programs to require recipients to spend at least 7.5 percent of their awards on improving their cybersecurity.[79] This requirement was added to State Homeland Security Program (SHSP) grants, which received $415 million in FY 2021 , and Urban Area Security Initiative (UASI) grants, which received $615 million in FY 2021 .[80] State and local recipients of these grants can use the funding to conduct cybersecurity training and planning, cybersecurity risk assessments, and improve their critical infrastructure's cybersecurity.[81] In addition, in FY 2021, when FEMA's Port Security Grant Program (PSGP) offered $100 million in assistance to state and local governments, applicants were slated to receive a 20 percent increase in their scores for addressing Cybersecurity National Priority Areas.[82] PSGP is part of a broader FEMA effort to help protect transportation infrastructure against potential terrorist attacks.[83]

---

[74] Coast Guard, "Cyber Strategic Outlook," p. 7.
[75] Id. at p. 28.
[76] Coast Guard, "Cyber Strategic Outlook," p. 32.
[77] Kimberly Underwood, "Coast Guard Embarks on Cyber Offense," AFCEA, (October 2021), available at https://www.afcea.org/content/coast-guard-embarks-cyber-offense
[78] Doubleday, "Coast Guard looks to plug digital holes," Federal News Network, August 4, 2021, available at https://federalnewsnetwork.com/cybersecurity/2021/08/coast-guard-looks-to-plug-digital-holes-in-maritime-infrastructure-under-new-cyber-outlook/
[79] FEMA Press Release, "DHS Announces Funding Opportunity for $1.87 Billion in Preparedness Grants," February 25, 2021, available at https://www.fema.gov/press-release/20210225/dhs-announces-funding-opportunity-187-billion-preparedness-grants
[80] Id.
[81] Id.
[82] FEMA – Port Security Grant Program Frequently Asked Questions, "Fiscal Year 2021 Port Security Grant Program," (February 25, 2021), available at https://www.fema.gov/sites/default/files/documents/FEMA_FY2021-PSGP-FAQ_02-18-21.pdf
[83] Id.

Environmental Protection Agency (EPA)

The EPA provides several cybersecurity services to state and local governments to help protect wastewater facilities.[84] These services include an online briefing to help state's assess cyber risks, a cybersecurity incident action checklist, training and response exercises, a Water Sector Cybersecurity Technical Assistance Provider Program to train state and regional water sector technical assistance providers, an online Vulnerability Self-Assessment Tool, and tools for the development of a tabletop exercise for cybersecurity incidents.[85]

Transportation Security Administration (TSA)

As a component agency of DHS since its creation in November 2001, the TSA states its mission is to "protect the nation's transportation systems to ensure freedom of movement for people and commerce."[86] In a constantly changing threat environment, TSA now prepares for cyber-related events like physical threats, as expressed in its 2018 TSA Cybersecurity Roadmap.[87] The roadmap provides the framework for how TSA can operate in the cyber environment, ensuring the protection of its data and information technology systems and ensuring the protection and resilience of the Transportation Systems Sector.[88] In line with that framework, TSA has moved to mandate certain protections and incident reporting requirements in response to recent cyberattacks.[89]

In addition to addressing longstanding cybersecurity vulnerabilities in the nation's private pipeline system, TSA must also address its own cyber weaknesses that increase the vulnerability of the nation's pipelines. In July 2021, GAO highlighted that additional pipeline-related weaknesses remain in TSA's internal policies.[90] These weaknesses include (1) incomplete information in TSA's pipeline risk assessments used to prioritize pipeline security reviews; and (2) aged protocols for responding to pipeline security incidents that TSA had not revised since 2010.[91] TSA officials concurred with GAO recommendations in this area and anticipate updating their policies and guidelines over the next year.[92] As TSA considers future directives mandating private sector action

[84] EPA, "EPA Cybersecurity Best Practices for the Water Sector," available at https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector
[85] Id.
[86] TSA, "Mission," available at https://www.tsa.gov/about/tsa-mission
[87] TSA, "TSA Cybersecurity Roadmap 2018" (November 2018), p 2, available at https://www.tsa.gov/sites/default/files/documents/tsa_cybersecurity_roadmap_adm_approved.pdf#:~:text=TSA%E2%80%99s%20mission%20responsibilities%20include%3A%20%281%29%20securing%20its%20own,in%20coordination%20with%20DHS%20to%20secure%20its%20cyberspace
[88] Id.
[89] DHS, "DHA Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," (May 2021), available at https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators; see e.g., Holland and Knight, "TSA's Pipeline of Cybersecurity Requirements," (August 2021), available at https://www.jdsupra.com/legalnews/tsa-s-pipeline-of-cybersecurity-5827015/#:~:text=At%20a%202019%20joint%20congressional,against%20an%20evolving%20threat%20environment
[90] GAO, "TSA is Taking Steps to Address Some Pipeline Security Program Weaknesses," (July 2021), available at https://www.gao.gov/assets/gao-21-105263.pdf
[91] Id.
[92] Id.

related to critical infrastructure, it is incumbent on TSA to maintain maximum credibility by fixing and updating its own cybersecurity policies and processes quickly and thoroughly.[93]

In October 2021, the Department of Justice (DOJ) announced that DOJ may seek substantial fines on government contractors or companies that receive federal funds when they fail to follow TSA cybersecurity standards by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches.[94]

Cybersecurity and Infrastructure Security Agency (CISA)

The CISA is a component agency of DHS and leads national cybersecurity and infrastructure security efforts.[95] CISA helps protect the federal government's computer networks and partners with stakeholders in the public and private sectors to help improve cybersecurity and resiliency.[96] CISA also offers various services to stakeholders, including infrastructure assessments and analysis, information sharing between the public and private sector, training and exercises, and coordination of situational awareness and response to national cyber incidents.[97]

However, CISA's actions in some areas have been criticized.[98] For instance, CISA is responsible for the safety, security, and resiliency of the more than 91,000 dams nationwide, 63 percent of which are privately owned.[99] Dams are vulnerable to cybersecurity threats.[100] In 2016, the DOJ charged seven hackers linked to the Iranian government with carrying out a coordinated large scale cyberattack against dozens of banks and a small dam outside New York City.[101] In September 2021, the DHS OIG evaluated CISA's oversight of the Dams Sector and warned, "when they fail, the effects create a cascade of water inundation and flooding to buildings and agriculture, loss of power, disruptions to transportation, and damage to communication lines."[102] The report found that CISA does not manage or evaluate its Dams Sector activities, does not coordinate or track its own

---

[93] See, e.g., Michael Hudson, "What if the Threat Comes from Within? Federal Agencies Must Address the Risk," The Hill (June 2021), available at https://thehill.com/opinion/cybersecurity/557460-what-if-the-threat-comes-from-within-federal-agencies-must-address

[94] Gevena Sands, "TSA to impose cybersecurity on railroads and aviation industries," CNN, (October 2021), available at https://www.cnn.com/2021/10/06/politics/tsa-cybersecurity-mandates-railroad-aviation/index.html

[95]Brian E. Humphreys, "Critical Infrastructure: Emerging Trends and Policy Considerations for Congress," Congressional Research Service, July 8, 2019, available at https://www.everycrsreport.com/files/20190708_R45809_54416d7b2f43d41696e8e971832aea5fe96a9919.pdf

[96] CISA web site, "About CISA," available at https://www.cisa.gov/about-cisa

[97] CISA Services Catalog, p. 11, available at https://www.cisa.gov/sites/default/files/publications/FINAL_CISA%20Services%20Catalog%20v1.1_20201029_508_0.pdf

[98] Department of Homeland Security Office of Inspector General, "CISA Can Improve Efforts to Ensure Dam Security and Resilience," (September 9, 2021), pp. 5-10, available at https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-59-Sep21.pdf

[99] Id.

[100] Ryan Schoolmeesters, "Lessons Learned From Dam Incidents and Failures," Association of State Dam Safety Officials, (Undated), available at https://damfailures.org/lessons-learned/site-security-is-critical/

[101] "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," U.S. Department of Justice, (March 24, 2016), available at https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged

[102] Id.

Dams Sector activities, does not gather or evaluate performance information on Dams Sector activities, does not consistently coordinate and effectively communicate with FEMA and other external Dams Sector partners and stakeholders, and has not updated overarching critical infrastructure plans.[103] The agency concurred with the five recommendations the report made to improve CISA's oversight of the Dams Sector.[104]

Chronology of Recent Federal Government Actions on Cybersecurity

Obama Administration

- **Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity.** This EO was issued by President Obama on February 12, 2013,[105] and designed to improve critical infrastructure's ability to manage cyber risks.[106] The EO sought to foster information sharing, promote the adoption of cybersecurity practices, and tasked the National Institute of Standards and Technology (NIST) with working with the private sector to identify voluntary standards and industry best practices in order to develop a voluntary Cybersecurity Framework whose adoption would help organizations enhance their cybersecurity preparedness and lower their risk of falling victim to cyberattacks.[107]

- **Presidential Policy Directive (PPD) 21 – Critical Infrastructure Security and Resilience.** This PPD was published in conjunction with EO 13636 on February 12, 2013, replaced an earlier PPD on critical infrastructure, and established a national policy on critical infrastructure security.[108] The PPD directed agencies to develop a situational awareness capability, understand the consequences of infrastructure failures, mature public-private partnerships, and update the National Infrastructure Protection Plan.[109]

Trump Administration

- **EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.** This EO was issued by President Trump on May 11, 2017 and designed to

---

[103] Department of Homeland Security Office of Inspector General, "CISA Can Improve Efforts to Ensure Dam Security and Resilience," (September 9, 2021), pp. 5-10, available at https://www.oig.dhs.gov/sites/default/files/assets/2021-09/OIG-21-59-Sep21.pdf

[104] Id.

[105] Federal Register, "Executive Order 12636 Improving Critical Infrastructure Cybersecurity," (February 12, 2013), available at https://www.federalregister.gov/documents/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity

[106] The White House (Obama Administration), "Cybersecurity – Executive Order 13626," available at https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity/eo-13636

[107] The White House (Obama Administration), "Executive Order – Improving Critical Infrastructure Cybersecurity," (February 12, 2013), available at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

[108] CISA, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," available at https://www.cisa.gov/homeland-security-presidential-directive-7; The White House (Obama Administration), "Presidential Policy Directive – Critical Infrastructure 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

[109] CISA, "EO 13636 and PPD 21 Fact Sheet," (March 2013), available at https://www.cisa.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf

enhance "the security of federal networks and critical infrastructure."[110] Notably, the EO indicated that the president would hold agencies "accountable for managing cybersecurity risk to their enterprises."[111] It also empowered the DHS Secretary to serve "as the nation's key coordinator for all aspects of critical infrastructure security, including cybersecurity."[112]

- **EO 13833, Enhancing the Effectiveness of Agency Chief Information Officers.** This EO was issued on May 15, 2018, by President Trump and empowered agency chief information officers (CIOs) by increasing their scope of authority, especially regarding agencies' IT management.[113]

- **National Maritime Cybersecurity Plan to the National Strategy for Maritime Security.** Published in December 2020, this plan was meant to integrate cybersecurity into the National Strategy for Maritime Security (NSMS).[114] The plan committed to setting standards to mitigate risks in the maritime sector, promote information sharing, and build a cyber workforce.[115] The 2020 plan followed President Trump designating the Maritime Transportation System (MTS)[116] a "top priority" in the 2017 National Security Strategy.[117]

- **Cyberspace Solarium Commission.** This commission is a bipartisan and intergovernmental body created by the *John S. McCain National Defense Authorization Act for Fiscal Year 2019* with the purpose to develop a strategic approach to defense against significant cyberattacks.[118] The Commission published its report in March 2020 and was reauthorized in the *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*.[119]

---

[110] The White House (Trump Administration), "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017, available at https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

[111] Id.

[112] National Security Archive, "President Trump's Executive Orders on Critical Infrastructure," available at https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-10-22/president-trumps-executive-orders-critical-infrastructure

[113] The White House (Trump Administration), "President Donald J. Trump is Enhancing the Effectiveness of Agency Chief Information Officers," May 15, 2018, available at https://trumpwhitehouse.archives.gov/briefings-statements/president-donald-j-trump-enhancing-effectiveness-agency-chief-information-officers/

[114] The White House (Trump Administration), "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security," (December 2020), available at https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/12.2.2020-National-Maritime-Cybersecurity-Plan.pdf; Homeland Security Digital Library, "National Maritime Cybersecurity Plan Released," (January 12, 2021), available at https://www.hsdl.org/c/national-maritime-cybersecurity-plan-released/

[115] The White House (Trump Administration), "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security," (December 2020); Homeland Security Digital Library, "National Maritime Cybersecurity Plan Released," (January 12, 2021), available at https://www.hsdl.org/c/national-maritime-cybersecurity-plan-released/

[116] The Maritime Transportation System (MTS) includes the nation's waterways, ports, and land-side connectors, additional information available at https://www.maritime.dot.gov/outreach/maritime-transportation-system-mts/maritime-transportation-system-mts

[117] The White House (Trump Administration), "Statement from National Security Advisor Robert C. O'Brien Regarding the National Maritime Cybersecurity Plan," (January 5, 2021), available at https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-robert-c-obrien-regarding-national-maritime-cybersecurity-plan/

[118] "Cyberspace Solarium Commission," available at https://www.solarium.gov/

[119] Id.

Biden Administration

- **Industrial Control Systems Cybersecurity Initiative.** This initiative, launched in April 2021, aims to improve the security of operational technology (OT) and industrial control systems (ICS) through the development and deployment of OT/ICS cyber monitoring technologies.[120] The initiative also started a pilot program to improve cybersecurity of the electricity infrastructure, a "100-Day plan," with aggressive milestones, which is led by the Department of Energy, in coordination with CISA.[121]

- **Cybersecurity Sprints.** CISA began a series of cybersecurity-focused "60-day sprints" in April 2021, the first focused on ransomware, with the following sprints focused on the cybersecurity workforce, ICS resilience, transportation security, election security, and international partnerships.[122] The sprints aim to remove roadblocks, elevate existing cybersecurity efforts, and launch new efforts, with the first sprint on ransomware to include an awareness campaign and engagement with industry.[123] The 60-day sprints and the 100-day plan are part of the Biden Administration's increased focus on cybersecurity issues.[124]

- **EO 14028, Improving the Nation's Cybersecurity**. This EO was issued by President Biden on May 12, 2021,[125] and is intended to improve cybersecurity by modernizing the defense of federal networks by moving to secure cloud services and a zero-trust architecture, improving information sharing by removing contractual barriers, and strengthening response capabilities.[126] It also calls for the creation of a Cybersecurity Safety Review Board, modeled after the National Transportation Safety Board, that would examine significant cybersecurity incidents in order to help apply lessons learned from these incidents and improve the nation's cybersecurity defenses.[127]

---

[120] Department of Energy, "Progress Report: 100 Days of the Biden Administration's Industrial Control Systems (ICS) Cybersecurity Initiative and Electricity Subsector Action Plan," (August 16, 2021), available at https://www.energy.gov/articles/progress-report-100-days-biden-administrations-industrial-control-systems-ics

[121] Id.

[122] Justin Katz, "Mayorkas announces cyber 'sprints' on ransomware, ICS, workforce," (March 31, 2021), available at https://fcw.com/articles/2021/03/31/mayorkas-cyber-sprints-speech.aspx; Jory Heckman, "DHS launching 60-day sprints ahead of upcoming executive order," (March 31, 2021), available at https://federalnewsnetwork.com/cybersecurity/2021/03/dhs-launching-60-day-cyber-sprints-ahead-of-upcoming-executive-order/

[123] DHS, "Secretary Mayorkas Outlines His Vision for Cybersecurity Resilience," (March 31, 2021), available at https://www.dhs.gov/news/2021/03/31/secretary-mayorkas-outlines-his-vision-cybersecurity-resilience

[124] Id.

[125] Federal Register, "Executive Order 14028 Improving the Nation's Cybersecurity," (May 12, 2021), available at https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[126] The White House, "Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity 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/

[127] Id.

- **TSA emergency security directives for the pipeline industry.** TSA issued two emergency security directives due to the May 2021 Colonial Pipeline ransomware attack.[128] The first, issued in May 2021, required pipeline companies to report cyber incidents to TSA and CISA, both part of DHS, and to name a cybersecurity point person; the second directive, issued in July 2021, required companies to develop an incident response plan for potential cyberattacks and implement specific mitigation measures to protect against ransomware attacks.[129]

- **National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems.** This memorandum was issued by President Biden on July 28, 2021,[130] and directed CISA and NIST to develop cybersecurity performance goals[131] and formally established the "Industrial Control Systems Cybersecurity Initiative."[132] The Initiative is a voluntary and collaborative effort between federal partners and critical infrastructure owners and operators to improve collaboration and increase the use of new cybersecurity technologies.[133] The Initiative was first launched earlier in April 2021 (see above) with the pilot program focused on the electricity subsector, with initiatives focused on the water and wastewater sector and the chemical sector to follow.[134]

- In October 2021, TSA announced plans for an additional **directive to address cybersecurity in the rail and aviation sectors**.[135] Reportedly, TSA will require higher-risk railroad and rail transit entities to report cyber incidents to the federal government, identify cybersecurity point persons, and put together contingency and recovery plans in case they become victims of cyberattacks.[136] For the airline industry, TSA will reportedly require critical U.S. airport operators, passenger aircraft operators, and all-cargo aircraft operators to designate cybersecurity coordinators and report cyber incidents to CISA.[137]

---

[128] Ellen Nakashima, "TSA to impose cybersecurity mandates on major rail and subway systems," The Washington Post, (October 6, 2021), available at https://www.washingtonpost.com/national-security/rail-cybersecurity-dhs-regulations/2021/10/06/b3db07da-2620-11ec-8831-a31e7b3de188_story.html

[129] Ellen Nakashima and Lori Aratani, "DHS to issue first cybersecurity regulations for pipelines after Colonial hack," The Washington Post, (May 25, 2021), available at https://www.washingtonpost.com/business/2021/05/25/colonial-hack-pipeline-dhs-cybersecurity/; *See also:* DHS Press Release, "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," July 20, 2021, available at https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

[130] The White House, "Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure," (July 28, 2021), available at https://www.whitehouse.gov/briefing-room/press-briefings/2021/07/28/background-press-call-on-improving-cybersecurity-of-u-s-critical-infrastructure/

[131] NIST, "White House National Security Memo Issued | NIST & DHS Developing Cybersecurity Performance Goals for Critical Infrastructure Control Systems," (July 29, 2021), available at https://www.nist.gov/news-events/news/2021/07/white-house-national-security-memo-issued-nist-dhs-developing-cybersecurity

[132] The White House, "Background Press Call on Improving Cybersecurity of U.S. Critical Infrastructure."

[133] 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/

[134] Id.

[135] Ellen Nakashima, "TSA to impose cybersecurity mandates on major rail and subway systems," The Washington Post.

[136] Id.

[137] Maggie Miller, "TSA to issue regulations to secure rail, aviation groups against cyber threats," The Hill, (October 6, 2021), available at https://thehill.com/policy/cybersecurity/575580-tsa-to-issue-regulations-to-secure-rail-aviation-groups-against-cyber

- The recently enacted bipartisan ***Infrastructure Investment and Jobs Act***, (P.L. 117-58) provides approximately $2 billion "to modernize and secure federal, state, and local IT and networks; protect critical infrastructure and utilities and support public or private entities as they respond to and recover from significant cyberattacks and breaches."[138]

[138] Public Law No: 117-58, :Infrastructure Investment and Jobs Act, Congress.gov; White House Fact Sheet, "Top 10 Programs in the Bipartisan Infrastructure Investment and Jobs Act That You May Not Have Heard About, (August 3, 2021), available at https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/03/fact-sheet-top-10-programs-in-the-bipartisan-infrastructure-investment-and-jobs-act-that-you-may-not-have-heard-about/

WITNESS LIST

Mr. Cordell Schachter
Chief Information Officer (CIO)
Department of Transportation (DOT)

Mr. Larry Grossman
Chief Information Security Officer (CISO)
Federal Aviation Administration (FAA)

Ms. Victoria Newhouse
Deputy Assistant Administrator for Policy, Plans, and Engagement
Transportation Security Administration (TSA)

Rear Admiral John W. Mauger
Assistant Commandant for Prevention Policy (CG-5P)
U.S. Coast Guard (USCG)

Mr. Kevin Dorsey
Assistant Inspector General for Information Technology Audits
Office of Inspector General (OIG)
Department of Transportation (DOT)

Mr. Nick Marinos
Director
Information Technology and Cybersecurity
Government Accountability Office (GAO)