CSC 2.0

June 2023

Revising Public-Private Collaboration to Protect U.S. Critical Infrastructure

The Review of PPD-21 is an Opportunity to Revitalize Sector Risk Management Agencies

Mary Brooks, Annie Fixler & RADM (Ret.) Mark Montgomery

Table of Contents

Executive Summary

Few things more directly impact Americans' security and well-being than the reliability, availability, and safety of critical infrastructure. The security of this critical infrastructure relies, in turn, on the strength of the relationship between the government and the private sector, which owns and operates the majority of the infrastructure. Thus, the federal government has endeavored for decades to build a strong relationship with the private sector.

Nevertheless, the policy underpinning this public-private sector relationship has become outdated and incapable of meeting today's demands. Similarly, the implementation of this policy — and the organization, funding, and focus of the federal agencies that execute it — is inadequate. This report will evaluate the state of the public-private sector relationship and offer recommendations to reshape it to improve national security going forward.

Fuel holding tanks at Colonial Pipeline's Dorsey Junction Station in Woodbine, Maryland. (Photo by Drew Angerer/Getty Images)

The timing could not be better. In late 2022, the Biden administration announced its intention to rewrite the Obama-era Presidential Policy Directive 21 (PPD-21), which established the current iteration of the critical infrastructure protection framework. This decision followed congressional intervention two years earlier to clarify and expand the role of federal agencies responsible for interfacing with the private sector.[1] Congress designated these organizations as Sector Risk Management Agencies (SRMAs) — there is at least one for each of the 16 sectors of U.S. critical infrastructure. It also ordered the Department of Homeland Security (DHS) to review the SRMAs' performance and recommend improvements.

Before deciding to revamp PPD-21, the Biden administration conducted assessments of the federal government's authorities to regulate security standards for critical infrastructure[2] and launched a number of targeted, high-visibility efforts to address sector-specific problems and draw attention to cybersecurity issues. Additionally, the Biden administration has issued executive orders and national security memoranda intended to strengthen federal cybersecurity and lay out voluntary cybersecurity performance goals for critical infrastructure providers. The administration also established congressionally mandated public advisory committees to evaluate critical infrastructure protection.[3] The creation of the Office of the National Cyber Director, meanwhile, has provided improved strategic coordination across the interagency and with private sector stakeholders.

This incremental approach, however, is not delivering the necessary improvements to SRMA performance, especially as both physical and — especially — cyber threats to the country's critical infrastructure continue to escalate.

As the administration begins its review process, it should focus specifically on improving the relationship between the public and private sectors — by making government a better partner to industry and through both voluntary partnerships and regulation, as noted in the new National Cybersecurity Strategy.[4] This report identifies flaws in both the design and implementation of public-private collaboration policy and argues that these flaws are amplified by discrepancies in the structure, resourcing, and capabilities of SRMAs. In short, the performance of SRMAs is inconsistent at best and wholly deficient at worst.

Meanwhile, there are numerous other challenges. The strategy and policy documents governing critical infrastructure have become stale. The current systems for designating sectors as critical and for mitigating cross-sector risks are inadequate. DHS's Cybersecurity and Infrastructure Security Agency (CISA) is unable to fulfill its responsibilities, and it does not receive the interagency support necessary to act effectively as the national risk manager. Voluntary security relationships are not delivering the necessary results. Additionally, processes for sharing information, responding to emergencies, designating priority infrastructure within sectors, and promoting resilience are insufficient.

Despite these challenges, this report concludes that the overall concept underlying the government's critical infrastructure protection system — anchored in an approach that balances regulation, incentivization, and collaboration — remains the best method to coordinate the public and private sectors. The report offers operational-level recommendations to improve the existing system while addressing broader strategic considerations that require an update to PPD-21. It also offers specific guidelines on how to revise PPD-21 to preserve what is working while also addressing the significant challenges in building effective public-private collaboration.

Recommendations

Rewrite PPD-21 for a New Era

1. Clearly identify strategic changes
2. Assign responsibilities and ensure accountability for routine updates of key strategic documents
3. Clarify CISA's roles and responsibilities as national risk management agency (NRMA)
4. Resolve questions around the organization and designation of critical infrastructure sectors and assigned SRMAs
5. Provide guidance on SRMA organization and operation
6. Facilitate accountability

Support the PPD-21 rewrite with implementation and resourcing efforts

7. Strengthen CISA's capabilities to execute its NRMA responsibilities
8. Resource SRMAs for their responsibilities
9. Identify a more effective way to catalog, support, and protect priority infrastructure
10. Develop functional information-sharing capacity across all sectors
11. Organize public-private collaboration to mitigate systemic and cross-domain risk
12. Ensure effective emergency response

Railroad switching yard in Illinois. (Photo by Jonathan Kim/Getty Images)

Acronyms

Cybersecurity and Infrastructure Security Agency	CISA
Department of Energy	DOE
Department of Homeland Security	DHS
Department of Transportation	DOT
Electricity Information Sharing and Analysis Center	E-ISAC
Environmental Protection Agency	EPA
Federal Aviation Administration	FAA
Federal Energy Regulatory Commission	FERC
Government Accountability Office	GAO
government coordinating council	GCC
Information Sharing and Analysis Center	ISAC
Joint Collaborative Environment	JCE
national critical functions	NCF
National Defense Authorization Act	NDAA
National Infrastructure Protection Plan	NIPP
national risk management agency	NRMA
National Risk Management Center	NRMC
North American Electric Reliability Corporation	NERC
Office of Cybersecurity, Energy Security, and Emergency Response	CESER
Presidential Policy Directive	PPD
sector coordinating council	SCC
sector risk management agency	SRMA
sector-specific agency	SSA
sector-specific plan	SSP
systemically important critical infrastructure	SICI
systemically important entities	SIEs
Transportation Security Administration	TSA

Organization of the Sector Risk Management Agency (SRMA) Framework

Two Obama-era directives created the foundation of the critical infrastructure protection framework in use today: Presidential Policy Directive 21 (PPD-21) and Executive Order (EO) 13636. These directives built on work done in the Bill Clinton and George W. Bush administrations, including efforts to establish a cross-sector critical infrastructure protection commission[5] and assign lead agencies to work with designated sectors of U.S. infrastructure.[6]

The Obama administration issued the first of these directives, PPD-21, "Critical Infrastructure Security and Resilience," on February 12, 2013, focusing on improving critical infrastructure security and resilience (both physical and cyber).[7] PPD-21 established strategic goals for critical infrastructure protection, designated 16 critical infrastructure sectors — the same 16 that remain designated today[8] — and assigned to each a sector-specific agency (SSA). Each SSA was to serve as the federal interface for its sector, support incident management, facilitate the identification and mitigation of vulnerabilities, and share information with DHS. The directive tasked DHS itself with supporting all SSAs and coordinating the federal government's overall approach to critical infrastructure security and response to significant cyber or physical incidents. PPD-21 also tasked DHS with serving as national risk manager, a role now played by the department's Cybersecurity and Infrastructure Security Agency, or CISA.

Presidential Policy Directive 21 established strategic goals for critical infrastructure protection, designated 16 critical infrastructure sectors — the same 16 that remain designated today — and assigned to each a sector-specific agency.

PPD-21 also mandated an update to the National Infrastructure Protection Plan (NIPP), which had last been updated four years prior.[9] The updated NIPP required each SSA to develop a sector-specific plan (SSP) outlining the sector's unique operational and threat landscape and setting priorities for addressing risks.[10] Accordingly, each SSA published a 2015 SSP.[11] However, no federal agency has updated its 2015 SSP, despite the NIPP's requirement to update them every four years.

The second key directive, EO 13636, focused on improving the cybersecurity of critical infrastructure, in particular by creating more robust engagement and information sharing between stakeholders, including government coordinating councils (GCCs) and sector coordinating councils (SCCs).[12] GCCs include government stakeholders from federal, state, local, tribal, and territorial governments, while SCCs are industry-led. SCCs are "self-organized, self-run, and self-governed" and "serve as principal entry points for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues."[13] EO 13636 also began the development of a baseline cybersecurity framework for critical infrastructure.

Additionally, Section 9 of EO 13636 required the secretary of homeland security to identify the most critical of critical infrastructure — entities against which a successful attack would lead to catastrophic national security, economic security, or public health consequences.[14] The list of "Section 9 entities" consists largely of financial institutions, electricity providers, and telecommunications companies.[15]

While PPD-21 and EO 13636 exert a decisive influence on the organization, governance, and performance of public-private collaboration, other presidential directives also shape the critical infrastructure protection system. For example, PPD-8, another Obama-era directive, assigns responsibilities and sets goals for national preparedness to prevent, respond to, and recover from natural disasters and man-made attacks.[16] PPD-41, meanwhile, governs the federal government's coordination in the event of a major cyberattack.[17]

The framework established by PPD-21 and EO 13636 a decade ago remains in place today, with one significant update. On the recommendation of the congressionally mandated Cyberspace Solarium Commission, Congress elevated the departments and agencies responsible for coordination with critical infrastructure owners and operators,[18] redesignating SSAs as SRMAs, establishing their roles in law, and assigning them additional duties to support risk management and incident response. The law outlined SRMA responsibilities and requirements more explicitly, clarifying some and adding others — such as the need to assess risk and support emergency planning and preparedness.

According to Section 9002 of the fiscal year (FY) 2021 National Defense Authorization Act (NDAA), SRMAs are required to:

1. **support sector risk management**, including by creating programs that help critical infrastructure owners and operators identify and mitigate threats and other risks to their systems or assets, and by recommending ways to minimize the impact of attacks if they occur;
2. **assess sector risk**, including by evaluating and prioritizing physical and cyber-related threats and by supporting the national risk assessment efforts of DHS;
3. **manage sector coordination**, including serving as the federal government interface for sector activities, serving as the federal GCC chair, and participating in cross-sector coordinating councils;
4. **facilitate information sharing** with DHS and other federal entities regarding physical and cyber threats by facilitating bi-directional information sharing between government and industry, working with critical infrastructure owners and operators to identify their needs and priorities, sharing in real time — to the extent possible — threats or other key security-related actions, and providing information to DHS to meet reporting requirements;
5. **support incident management**, including incident response efforts and restoration efforts — upon request and in coordination with CISA — in national cybersecurity asset response activities; and
6. **contribute to emergency preparedness efforts**, including by working with DHS and critical infrastructure owners and operators to develop response plans for physical and cyber crises and supporting exercises to prepare and conduct said events.[19]

While the responsibilities of SRMAs are consistent across sectors, the sectors themselves are often very different. Some — like water and wastewater — consist of a highly decentralized network of tens of thousands of different systems. Others include a much smaller number of assets. Several of the sectors have internal divisions or sub-elements, referred to inconsistently as "subsectors" or "disciplines," "segments," or "components" in SSPs. For example, the energy sector has two designated subsectors: 1) electricity and 2) oil and natural gas, each with its own subsector coordinating council and corresponding GCC. The transportation sector, in contrast, has seven subsectors, including pipelines that transport oil and natural gas products across the United States (as well as other materials, such as water and chemicals). Appendix A lists the 16 sectors, their respective SRMAs, and the responsible office or sub-office within that SRMA as well as the sectors' various sub-elements.

Neither PPD-21 nor the FY 2021 NDAA provides specific guidance to federal agencies on how to manage or resource their SRMA responsibilities. The agencies may designate a specific office to execute the role of SRMA on behalf of the department. The SRMA for a given sector may or may not have regulatory authority over that sector, as discussed below.

In section 9002(b) of the FY 2021 NDAA, Congress tasked the secretary of homeland security with assessing the existing framework as well as the performance of SRMAs and, as applicable, issuing recommendations for 1) revising that framework, 2) the current list of sectors and their SRMAs, and 3) identifying and designating new sectors or subsectors. CISA conducted this assessment and transmitted its findings to the White House in November 2021.[20] Its report focused on weaknesses in the SRMA framework — with particular attention to CISA's own performance — and proposed concrete recommendations to improve the system. In November 2022, the Biden administration forwarded the DHS report to Congress and made the findings public.[21] Alongside the report, the White House issued a letter from President Joe Biden noting the administration's intent to revise PPD-21.[22]

Anatomy of a Crisis: The SRMA Framework and the Colonial Pipeline Breach

On May 7, 2021, the Russia-based cybercriminal gang DarkSide launched a ransomware attack against the corporate networks of Colonial Pipeline, the energy distributor responsible for shipping nearly half of the East Coast's gas and jet fuel. Colonial Pipeline, claiming it was unable to confirm whether the ransomware might compromise the security of its industrial control systems — and unable to bill its customers — took its system fully offline for several days.[23]

This incident illustrates the challenges faced by the national critical infrastructure system in a moment of crisis and the limits of the public-private partnership model that the government has tried to cultivate. The three most important lessons related to public-private collaboration from the Colonial Pipeline attack are:

1. There was a breakdown in government information sharing: In a cyber incident, the FBI has primary responsibility for threat response, while CISA has primary responsibility for asset response, including technical assistance and mitigation.

During a cyber incident, the SRMA is supposed to provide sector-specific context for cyber and physical interactions and recovery prioritization so that incident responders understand nuances or unique needs in the sector. In this case, the affected company was part of the pipeline subsector of the transportation sector for which the Transportation Security Administration (TSA) and the Department of Transportation serve as co-SRMAs. SRMAs are also supposed to facilitate information sharing, particularly between industry and government, and to help mitigate emergency incidents. However, neither PPD-21 nor PPD-41 practically defines how to do these things.[24]

Yet during the response to the Colonial Pipeline breach, information appears to have been siloed within government agencies. After detecting the breach, Colonial Pipeline informed the FBI of the cyberattack, yet according to the testimony of CISA officials, the FBI did not inform CISA of the crisis for several hours, and Colonial did not contact CISA separately.[25] (Brandon Wales, then CISA's acting director, testified that he did not believe Colonial would have notified CISA at all had the FBI not done so.)[26] And neither the FBI nor Colonial immediately notified the TSA or the Department of Transportation.

2. The SRMA framework struggled to be relevant during emergency response: As the co-SRMA for the pipeline subsector, the TSA has "primary oversight responsibility for the physical security and cybersecurity of pipeline systems."[27] However, the product carried in the pipeline — jet fuel and gasoline — is part of the energy sector. Simply put, supporting the security and resilience of the pipeline was the TSA's responsibility, but the Department of Energy (DOE) held responsibility for ensuring that the product was delivered.

In the Colonial Pipeline case, DOE appears to have served as the primary interagency coordinator for the federal government as a result of a White House decision.[28] By most accounts, DOE did an admirable job in this role, and, as the chief concern was less the security of the pipeline and more the availability of energy, there was a natural role for DOE. Nevertheless, it appears CISA and TSA were marginalized, which indicates at least some elements of the SRMA framework are not optimized for crisis response.

3. Pre-crisis collaboration and partnerships — particularly voluntary security standards, relationships, and processes — proved insufficient: At the time of the incident, Colonial Pipeline had no regulatory requirement to inform the government of a cyber breach, nor was the company required to meet specific cybersecurity standards.

TSA had previously issued voluntary security guidelines for pipelines and conducted security assessments of private pipeline companies in its role as SRMA.[29] TSA testified to Congress, however, that Colonial Pipeline declined several of its offers for physical security and cybersecurity assessments, although the company had participated in corporate security reviews and critical facility security reviews in the past.[30]

In the wake of the breach, TSA issued an emergency pipeline directive to compel incident reporting and designation of a central point of contact within companies.[31] Oil and natural gas industry associations and infrastructure cybersecurity experts criticized the first iteration of this directive not only as overly prescriptive but also as technically infeasible.[32] TSA has subsequently revised the directive multiple times with increasing industry input and support, although disagreements on substance and process remain between TSA and industry groups.[33] Additionally, in early 2022, Congress passed a new law, the "Cyber Incident Reporting for Critical Infrastructure Act of 2022," which will require critical infrastructure providers to report cyberattacks to CISA within 72 hours.

Inconsistent Performance Across SRMAs — Three Examples

The lessons learned from the Colonial Pipeline ransomware incident speak to the broader challenge of inconsistent capabilities and performance across SRMAs. While the FY 2021 NDAA attempted to rectify discrepancies by establishing consistent responsibilities, not all SRMAs have the necessary authorities and resources to perform their jobs well. Poor performance may also result from how the SRMA's responsibilities are delegated within the department or a lack of agency leaders' commitment to the SRMA's mission. The following examples detail the performances of 1) a mature, well-resourced SRMA, 2) a rapidly growing SRMA, and 3) an under-resourced SRMA, in three complex, distributed, and particularly important critical infrastructure sectors.

Energy

According to assessments by industry and government experts, the energy sector is one of the strongest performing sectors, and the DOE is one of the best performing SRMAs.[34] The energy sector has clear leadership from government and strong industry-led organizations. It is also well-resourced. This is very beneficial since PPD-21 defined energy as a "uniquely critical" sector, given how it powers all others.[35]

DOE exercises its SRMA role through the Preparedness, Policy, and Risk Analysis division of the Office of Cybersecurity, Energy Security, and Emergency Response (CESER). DOE chairs the energy sector GCC, with DHS serving as co-chair.[36] CESER is well-resourced, with dedicated funding and staff allocations for its cybersecurity, preparedness, and resiliency efforts. Notably, one expert we interviewed maintained that DOE has acquired robust resources because industry members have lobbied Congress to ensure sufficient appropriations — something that not all sectors are able or willing to do. CESER received some $200 million in the FY 2023 omnibus appropriations bill signed by President Biden in December.[37]

DOE is not a regulator for the energy sector. While the Federal Energy Regulatory Commission (FERC) serves as the industry's primary regulator, the secretary of energy can respond to crises — for example, a grid security emergency stemming from storm damage or a cyberattack — under authority granted by the Natural Gas Policy Act of 1978 and the Federal Power Act.[38] FERC also has the authority to issue emergency directives.

Critical infrastructure asset owners and operators throughout the sector have also invested heavily in resilience, risk mitigation, communication, and collaboration. This is particularly true within the electricity subsector. The Electricity Subsector Coordinating Council, for example, "consists of CEO level representatives."[39] Usually, senior executives, but not CEOs, serve on SCCs. This was a decision made by the SCC itself — not imposed by DOE — and it allows the council to quickly mobilize resources, implement decisions, and engage with government partners.

The electricity subsector also has one of the best Information Sharing and Analysis Centers (ISACs), according to industry experts.[40] ISACs are member-driven, information-sharing organizations that help connect the SRMA and the sector's companies and stakeholders. The Electricity ISAC (E-ISAC) hosts the biennial nationwide grid security exercise, GridEx. It also runs the Cybersecurity Risk Information Sharing Partnership, which facilitates bidirectional information sharing between industry and government.[41] The E-ISAC does not charge for general membership, which means it is open even to smaller or under-resourced entities that cannot pay. Most other ISACs, including the Oil and Natural Gas ISAC, charge for membership.[42]

The E-ISAC, however, is located within the North American Electric Reliability Corporation (NERC), a not-for-profit, industry-created regulatory organization that develops reliability and security standards for the bulk power system. While E-ISAC says it is "organizationally isolated from NERC's enforcement processes,"[43] our interviewees relayed that, because the E-ISAC is located within NERC, which, in turn, is subject to oversight by FERC, in-house counsels on occasion advise electricity companies not to share certain information with the ISAC for liability reasons. This is an obstacle without an obvious solution: removing the E-ISAC from NERC would likely strip it of key funding and relationships central to the services it provides to the sector.

Transportation

Transportation is arguably one of the most complicated sectors, with seven designated subsectors: aviation, highway and motor carrier, maritime transportation system, pipelines, mass transit and passenger rail, freight rail, and postal and shipping.

Transportation has two designated co-SRMAs: the Department of Transportation (DOT) and DHS. For all subsectors except maritime, DHS has assigned its SRMA responsibilities to TSA. The U.S. Coast Guard is the SRMA for the maritime subsector.[44] This is a rare circumstance in which the designated SRMA assigns different offices or agencies to handle subsectors within the same sector.

The Coast Guard collaborates with other government partners on seaport security, including with TSA on issues of perimeter security and worker credentialing.[45] For both rail subsectors, TSA coordinates with the Federal Railroad Administration. For the aviation sector, TSA serves as the SRMA but coordinates with the Federal Aviation Administration (FAA), in accordance with the Aviation and Transportation Security Act. The FAA also provides services and training for the aviation subsector and takes the lead on issues related to the security of airplanes themselves.[46]

For the pipeline subsector, TSA works in partnership with DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) to ensure the safe and secure operation of pipelines. TSA and PHMSA have regulatory authority and can issue emergency directives.[47] And since pipelines move crude oil, refined petroleum products, natural gas, petrochemicals, and other materials, many other sectors also have a stake in their security. As a result, there are growing efforts to promote cross-sector collaboration.[48]

Historically, TSA has fallen short in executing its SRMA duties, particularly for the pipeline subsector, according to successive reports from the Government Accountability Office (GAO).[49] DHS and DOT issued a "2018 Transportation Systems Sector Goals Progress Report" identifying areas of progress as well as ongoing challenges, including the need to improve engagement with the private sector.[50]

Since May 2021, TSA has attempted to improve its capabilities rapidly, though it is not yet a top-tier SRMA. In addition to the pipeline security directive, TSA has issued or is in the process of issuing similar emergency directives for the rail and aviation subsectors, although it has faced similar criticisms from those industries that the directives are technically or practically infeasible.[51] The co-SRMAs had a lot of "catching up to do" but were making security a priority, according to our interviews with industry stakeholders. While TSA had been under-resourced in the past, the agency has convinced Congress to provide greater funding.[52]

Water

Like the energy and transportation sectors, the water and wastewater systems sector is highly distributed. The sector includes approximately 52,000 drinking water and 16,000 wastewater systems, most of which serve fewer than 10,000 customers.[53] Unlike the other two sectors, water contains no subsectors, although drinking water utilities have different regulatory requirements from wastewater utilities.

Water has one designated SRMA: the Environmental Protection Agency (EPA). The EPA's Office of Water leads the agency's water sector resilience and cybersecurity efforts and performs SRMA functions. Two other EPA offices assist this effort: the Office of Homeland Security, which works with the intelligence community to facilitate information sharing and threat awareness regarding potential or actual cyberattacks, and the Office of Research and Development, which seeks to improve water utilities' abilities to prepare for and respond to all hazards that threaten public health. The EPA is also the regulatory agency for the water and wastewater sector as detailed in the American Water Infrastructure Act.

Water has a strong system of trade organizations. Water sector associations and the Water ISAC (itself managed by one of the associations, the Association of Metropolitan Water Agencies) have worked to improve cybersecurity in water utilities. As far back as 2008, the Water SCC's Cyber Security Working Group, supported by the American Water Works Association, produced a "Roadmap to Secure Control Systems in the Water Sector" and updated it in 2013 and 2017. The roadmap aimed to develop

and implement security programs and support risk management by utilities. These industry groups also provide web-based training, offer a comprehensive library of technical documents, and suggest best practices for water and wastewater utilities.

Despite these industry efforts, the water sector is one of the weakest in terms of cybersecurity. The sector has highly distributed, aging infrastructure increasingly controlled by automated systems. Many utilities are owned and operated by cities and localities that lack the resources to strengthen cybersecurity, and asset owners and operators tend to spend the limited funds available on lead pipe mitigation and preparation for natural disasters.

Government and industry do not have a sufficiently productive relationship in the water sector. There is no mechanism for collaboration to establish reliability and security standards, risk-based compliance, and regulations.

While owners and operators bear some responsibility for the sector's poor cybersecurity, an underlying cause is weak leadership and poor resourcing of the SRMA, for which both the EPA and Congress are to blame. Over the past 20 years, the EPA has not been organized or resourced to identify and support the sector's cybersecurity needs.[54] The Office of Water includes a cybersecurity element staffed by a handful of employees[55] and is vastly under-resourced for the tasks expected of an SRMA for a sector with nearly 70,000 utilities whose customer base is, of course, the entire population of the United States.

Government and industry do not have a sufficiently productive relationship in the water sector. There is no mechanism for collaboration to establish reliability and security standards, risk-based compliance, and regulations. EPA's efforts over the past two years to impose cybersecurity standards via existing assessments using state-level sanitary system checks have been met with significant industry pushback and complaints about a lack of engagement.[56] Congress, meanwhile, has not exercised sufficient oversight to ensure the EPA provides meaningful support to the water sector. Nor has it appropriated adequate resources to the EPA to, for example, administer grants and low-interest loans focused on cybersecurity, work with the sector to improve cybersecurity guidelines, or collaborate with federal partners (including CISA) that also support water utilities. In the FY 2023 appropriations cycle, Congress rejected the EPA's request for a new $25 million cybersecurity grant program.[57]

Findings: Assessing the SRMA Framework

When properly organized, implemented, and resourced, the SRMA framework can be the right mechanism to coordinate across the large and dynamic critical infrastructure environment in the United States. However, the framework has produced inconsistent, and at times unsatisfactory, results. While several individual SRMAs are effective, there are substantial weaknesses in the framework that undercut its efficiency.

Many of the shortcomings are well-documented by internal and external stakeholders. Government watchdogs — especially the GAO — have repeatedly identified major weaknesses in the critical infrastructure protection framework and have warned that the existing system risks failing the American people. Some of these studies focus specifically on CISA as national risk manager[58] and some on specific sector risk management agencies.[59] The GAO has chastised successive administrations for failing to address or implement dozens of its recommendations over the past decade.[60] These unheeded recommendations include tracking and reporting on compliance with security guidelines and standards, improving threat and information sharing, and addressing sector-specific vulnerabilities. CISA's 9002(b) report, meanwhile, highlighted areas in which implementation of the SRMA framework needs improvement and gave tactical recommendations to improve performance.

We have combined this existing public analysis with information from recent interviews with government and industry experts and stakeholders to lay out the most significant problems below. These are not simply problems in the implementation of the framework but also in its design. We identify 10 issues, focusing on gaps in strategic policy documents, poor performance by CISA and SRMAs, and shortcomings in prioritization and cross-sector risk management.

Shortcomings and Challenges to Collaboration

1. Strategy and policy documents are static and out of date.
2. Information and guidance are inconsistent or missing.
3. CISA can do more to lead as the national risk management agency.
4. SRMA performance is inconsistent across agencies.
5. Efforts to break down silos across critical infrastructure sectors are insufficient.
6. The process for updating the list of critical infrastructure sectors is moribund.
7. Voluntary partnerships are central to success but alone are not generating sufficient protection of national critical infrastructure.
8. Mechanisms for analyzing risk and prioritizing assets within different sectors are inadequate.
9. Information sharing is still a source of frequent complaints.
10. Efforts to implement resilience, continuity, and emergency response efforts are insufficient.

Strategy and Policy Documents Are Static and Out of Date

Many of the key strategy and policy documents that govern the critical infrastructure protection framework are outdated. Not only is PPD-21 a decade old, despite defining policy for a rapidly evolving field, the NIPP and the SSPs are also nearly a decade old, despite requirements to update them every four years.[61] In at least one instance, the GAO found that a designated subsector lead agency reported it had not updated its SSP "because CISA ha[d] not directed it to do so," despite the clear requirement in the NIPP and in the agency's own SSP.[62]

This problem has been recognized but not remediated. In 2017, the Trump administration tasked an interagency policy committee with inserting "conforming edits" into the NIPP, but that does not appear to have happened.[63] In 2018, DHS published revised joint national priorities for the NIPP but did not revise the document more broadly.[64]

Out-of-date documents create a situation in which the stated strategy does not reflect current practice — a problem several of our interviewees corroborated. Out-of-date strategic documents may reference obsolete agencies, and at least two of the offices originally designated by the NIPP to fill SRMA roles no longer exist. Today, some stakeholders cannot even agree on the number of subsectors in their sector, the definition of a subsector, or why it matters (or does not matter).[65]

Meanwhile, the sectors themselves and the cyber and physical threats they face have evolved substantially over the past eight years. The healthcare sector faces rapidly escalating cyber threats from ransomware actors; commercial space systems, which are not designated as critical infrastructure,[66] are increasingly vital to economic prosperity and national security; and the composition of the energy sector is shifting with the expansion of renewable, distributed energy resources.

The lack of updated information undercuts the ability of individual SRMAs to fulfill their responsibilities. For example, the GAO warned about CISA's shortcomings as the SRMA for the communications sector:

> ... the current 2015 plan lacks information on new and emerging threats to the Communications Sector, such as security threats to the communications technology supply chain, and disruptions to position, navigation, and timing services. Developing and issuing an updated plan would enable CISA to set goals, objectives, and priorities that address threats and risks to the sector, and help meet its sector risk management agency responsibilities.[67]

In 2020, CISA decided to update the NIPP,[68] and the GAO reported that CISA told it a revision would be published by December 31, 2021.[69] CISA, however, has no office responsible for implementing the NIPP, and more than a year after this deadline, it appears that the NIPP is on hold, possibly pending a rewrite of PPD-21. If PPD-21 must be revised first, it is likely that a new NIPP will not be produced until 2025 and new SSPs will not be produced until 2026.

Information and Guidance Are Inconsistent or Missing

Interviews with government and industry representatives confirm that information and guidance related to the organization, goals, and processes of the SRMA framework is either non-public or not easily accessible. At best, this makes it difficult to understand the existing landscape. At worst, these gaps promote confusion during a crisis.

For example, it is not clear how responsibilities are divided between co-SRMAs or between SRMAs and CISA. While the NIPP and SSPs identify SRMAs for each sector, their internal management and organization is a decision largely left to each SRMA, resulting in a complex and inconsistent web of responsibilities. It is not always known — even by other government entities — what authorities SRMAs have: hence the White House decision earlier this year to launch an assessment of the federal agency authorities around critical infrastructure security.[70]

At times, there has been a failure to take advantage of opportunities to clearly delineate goals, roles, and processes. For example, many of the SSPs issued at the end of the Obama administration appear to be "cut and paste" versions of a template SSP, with little to no sector-specific guidance. These serve mostly as a statement of purpose, identifying the sector's assets, risks, vulnerabilities, threats, dependencies, and general structure. They fall short, however, on describing processes — for example, how the SCCs function and work with the GCCs. Several of the SSPs lack goals and metrics sections, while others include metrics that cannot reasonably indicate any real level of improvement or security. For example, the Chemical SSP seeks to track metrics like "number of tours offered ... and attended," "number of information products and education training products developed," and "number of R&D gaps identified."[71] These may be indicators of effort, but they are not indicators of progress, security, or resilience.

CISA Can Do More To Lead as the National Risk Management Agency

In addition to serving as SRMA for eight of the 16 sectors, CISA is the national risk management agency (NRMA). It hosts the National Risk Management Center (NRMC) and serves as the national coordinator for critical infrastructure security and resilience.[72] CISA's most recent strategic plan identifies its mission as one that "supports the other SRMAs in their security and resilience efforts by assisting with the identification and management of risks and providing access to CISA capabilities and resources."[73]

However, CISA is not, in many cases, serving as the leader that most interviewees said was needed to realize the full potential of the SRMA framework. They noted how SRMAs have had to adapt on their own over the past decade across three presidential administrations and how the success or failure of different sectors has been a "personality-driven process" — with the more assertive or proactive SRMAs doing better than their counterparts.[74] CISA also seems to have deprioritized its non-cyber elements, including physical protection of critical infrastructure.

CISA is aware of these concerns. DHS concurred with the GAO's March 2022 findings that CISA should "improve priority setting, stakeholder engagement, and threat information sharing"[75] — though it has not done so. In its 9002(b) report, CISA did acknowledge the need to "mature" its role as the NRMA. CISA's forthcoming force structure assessment, which is statutorily required, may address how it plans to do that.

Interviewees made similar points. They particularly urged CISA to create a national risk register to better and more proactively identify, analyze, collate, and share information with interagency and industry partners. While CISA has partially done this, in practice, it has not had the desired impact on information sharing,[76] and it may be necessary to establish supplementary authorities.[77] Interviewees also recommended that CISA update all policy documents and instruct SRMAs to update their SSPs. In addition, interviewees from industry mentioned wanting CISA (or some other government entity) to ensure better interagency information sharing so that industry only has to communicate to the government once about a particular incident or piece of information.

To raise the baseline performance of government partners and increase CISA's ability to serve as NRMA, the Cyberspace Solarium Commission recommended not just the codification of sector-specific agencies as sector risk management agencies but also complementary legislation recognizing "CISA's lead role in national risk management." Specifically, the commission

called for legislation to "clarify roles and responsibilities" between SRMAs and CISA as well as appropriations to provide the resources necessary for both SRMAs and CISA to "act as mature, steadfast partners in overall national resilience efforts."[78] However, congressional action is still pending.

SRMA Performance Is Inconsistent Across Agencies

The performance of SRMAs varies significantly. Most recently, CISA's 9002(b) report identified a need to provide "greater consistency in resources and doctrine" to SRMAs.[79] Interviewees highlighted the following problem areas:

Resourcing: Interviewees and observers have expressed concern about the failure of Congress to provide adequate resources to agencies for SRMA activities. Stakeholders from the energy and transportation sectors believe their sectors have more resources — in terms of designated funding and employees — than several others in large part because their agency or industry partners specifically made the case for this to Congress.

Relatedly, though it is beyond the purview of this paper, critical infrastructure sectors themselves need adequate resourcing. The costs of protecting assets and systems from cyber and physical threats are high. While some of these costs are borne by industry, there are circumstances in which threat mitigation may require government grants — for example, replacing lead pipes in the water sector or upgrading outdated software in the elections subsector.

Private sector relationships: Some sectors have a robust, ongoing partnership between government and industry and among industry partners. Other sectors, however, struggle with collaboration and information sharing. They may have stakeholder groups that meet infrequently or may even view their own industry counterparts with suspicion. While some sectors, such as energy, have highly centralized SCCs that have participation from the biggest stakeholders, other SCCs have less impact and are less competent and mature. There is a sense among interviewees that much of a sector's success comes down to relationships between the various stakeholders. Sectors that foster more engagement during periods of regular operation are likely to perform better during crises.

Many of these relationships, however, are individual, not institutional. The federal government is more likely to consult well-known industry players when creating regulations or standards. Trusted contacts are more likely to be brought in during a crisis. This is not necessarily a bad thing, but it does mean that when individuals leave or retire, those relationships must be rebuilt. It also means it is easier to overlook or exclude players who are not well known. Sectors that can buck this trend and ensure continuity of relationships across personnel turnover tend to have well-funded associations (such as the Edison Electric Institute) that support the SCCs.

Authorities: Some SRMAs have greater authority than others to set regulations or standards, monitor compliance, convene key stakeholders, or issue emergency directives. The Biden administration has used several authorities to impose additional cybersecurity guidance or regulations on specific industries — such as the pipeline and aviation subsectors — particularly when voluntary approaches do not appear to have worked.

Many in government make the case — as articulated in the administration's new National Cybersecurity Strategy[80] — that more regulation is necessary to ensure minimum security standards are met.[81] Anecdotally, there does appear to be a correlation between higher levels of cybersecurity regulation within a sector and higher prioritization of cybersecurity. However, it is not clear that the SRMA *itself* needs to have regulatory authority to promote improved security outcomes, whether cyber or physical.

And, of course, many in industry claim that less, smarter, and more flexible regulation improves outcomes. They assert that regulations impose red tape, are duplicative, and prioritize compliance rather than outcomes. They further point out that many of the leading experts in their sector are employed within the industry — and not by the U.S. government, CISA, or the SRMA — and that they are routinely required by the government to conduct box-checking compliance exercises that are impractical or ineffective.

Leadership structure: The federal department listed in PPD-21 as the SRMA further designates an office, division, agency, or other entity to carry out related taskings. Often, however, this designation falls to an entity poorly suited to the role.

In several cases, departments have assigned the SRMA responsibility, with its inherent focus on external engagement, to a chief information officer, whose role is inherently internally focused. In other cases, departments have placed the SRMA responsibility in an office with only a handful of employees. Both situations make execution of the SRMA role — including industry engagement — more difficult. SRMAs are most effective when responsibilities are assigned to an externally focused office with sufficient resources and access to agency leadership.

Inconsistency and poor performance are problems not just for managing individual sectors but also for national risk management. As the Cyberspace Solarium Commission argued, for "the federal government to scale up its efforts and advance a deeper collaboration with the private sector on cybersecurity and resilience fundamentally depends on … [SRMA] maturity, ensuring their consistency across sectors, and empowering them to represent their sectors and fully integrate with national risk management efforts led by CISA."[82] A September 2022 report from CISA's resilience advisory subcommittee similarly noted that "varying levels of maturity across critical infrastructure sectors" and "underutilization of existing policy and regulatory approaches" hamper the improvement of national risk management.[83]

Efforts To Break Down Silos Across Critical Infrastructure Sectors Are Insufficient

Critical infrastructures are highly interdependent: for example, water systems require electricity and communications to operate, while energy generation requires water as a coolant. A single company, meanwhile, may operate across multiple sectors. The Alyeska Pipeline company in Alaska, for example, operates pipelines (a component of the transportation subsector) that move oil (a part of the energy sector) to the Port of Valdez (in the maritime transportation subsector).

Partly to mitigate this challenge, DHS has created several cross-cutting entities, coordinated through the Critical Infrastructure Partnership Advisory Council, to improve communication and collaboration across SRMAs, between industry and the government, and across different levels of government — federal, state, local, tribal, and territorial. These include: 1) the Critical Infrastructure Cross-Sector Council (private sector),[84] 2) the Federal Senior Leadership Council (federal government),[85] 3) the Regional Consortium Coordinating Council, and 4) the State, Local, Tribal, and Territorial Government Coordinating Council. However, these structures have not resolved the problem, with CISA's 9002(b) report urging better cross-sector coordination.

In parallel, to understand and prioritize across interdependencies, CISA's NRMC established a set of national critical functions (NCFs). These are a series of key functions or outputs of the government and private sector that are essential for national security, economic prosperity, and public health and safety. The functions include things like "generate electricity" and "supply water" as well as others like "preserve constitutional rights" and "provide public safety." CISA explains NCFs as a new "language" of infrastructure security,[86] designed to improve understanding of relationships and outcomes and help prioritize in times of crisis.

The reception of this effort outside of CISA has been mixed. The main shortcoming is that while NCFs are a good way to prioritize outputs, particularly during disaster recovery, they are not (nor were they intended to be) an organizational structure for ongoing collaboration between government and critical infrastructure asset owners and operators.

The Process for Updating the List of Critical Infrastructure Sectors Is Moribund

PPD-21 provides for additions or updates to the list of critical infrastructure sectors through an assessment by the DHS secretary in consultation with the assistant to the president for homeland security and counterterrorism. This process was used once, to add the elections infrastructure subsector to the government facilities sector in 2017, following Russian cyber-enabled information operations during the 2016 election cycle.[87]

This method of updating the list of critical infrastructure sectors appears to be ad hoc by design and is executed by fiat of the DHS secretary. There is no formal process within the NRMC[88] or elsewhere to designate, update, or remove sectors or subsectors.

This may change soon. Per the FY 2021 NDAA, DHS must review the designation of critical infrastructure sectors every five years and offer recommendations to revise the list. However, it is not yet clear what this process will look like in practice.

CISA's 9002(b) report does lay the groundwork for creating a standardized analytic process. The report, however, focused only on the criteria to determine whether an industry should be added, not on how to achieve interagency sign-off, ensure a timely process, and implement such a decision. Nor does the report directly address how a sector might be removed from the critical infrastructure list, how to assess whether PPD-21 assigned the appropriate department as SRMA, or, in the unique case of CISA, whether eight sectors are too many for a single agency to serve while also overseeing the SRMA framework.[89]

Voluntary Partnerships Are Central to Success, but Alone Are Not Generating Sufficient Protection of National Critical Infrastructure

The SRMA framework thrives or fails based on the quality of relationships and communication among industry, SRMAs, and CISA (as the NRMA). Regulation dictates some aspects of these interactions, but much of the public-private partnership is voluntary. Most notably, CISA is not a regulatory agency.

It appears that voluntary partnerships have reached their limits in recent years. While great work has been done in many sectors, there are others that have not prioritized security requirements and standards to the extent needed to protect industry assets and ensure critical infrastructure reliability. A mix of regulation, incentives, and improved collaborative processes will likely be needed for the infrastructure sectors that have relied on this voluntary process with limited to no success.

The Biden administration's new National Cybersecurity Strategy appears ready to change the balance in favor of stronger regulation. It says, "While voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has too often resulted in inadequate and inconsistent outcomes."[90]

Mechanisms for Analyzing Risk and Prioritizing Assets within Different Sectors Are Inadequate

A key responsibility for every SRMA is assessing and managing the risks in its sector. This involves prioritizing the security and resilience of the most important entities or assets (systemically important entities, SIEs, or systematically important critical infrastructure, SICI). However, existing prioritization efforts — of which there are several — are insufficient.

Under the National Critical Infrastructure Prioritization Program, CISA is tasked with creating an annually updated list of assets and systems whose loss would have catastrophic effects. However, a GAO report found that stakeholders, including at CISA, did not find this list useful.[91]

The NCFs, meanwhile, focus on the key functions that infrastructure provides rather than on companies or systems that provide those functions. As a result, they do not provide a usable list that would enable the U.S. government, for example, to prioritize the distribution of limited resources in a crisis.

Regarding the Section 9 prioritization in EO 13636 to identify the most critical of critical infrastructure, CISA's resilience advisory subcommittee concluded that the process was not useful and recommended that Section 9 be done away with entirely.[92] Similarly, the Cyberspace Solarium Commission, in its March 2020 report, noted that while the premise of Section 9 is correct — namely, that "not all critical infrastructure is of equal importance"[93] — it was not accomplishing what it was designed to do. CISA's advisory subcommittee recommended the creation of a new method for designating SIEs/SICI tied to the NCFs.[94]

Therefore, CISA's 9002(b) report, in a section on enhancing public-private collaboration, called for an interagency review assessing whether SRMAs and CISA need new authorities to identify SICI. The report determined that the secretary of homeland security and SRMAs should have the authority to "designate high-priority infrastructure, target federal resources to designated infrastructure, and require certain actions from owners and operators of such."[95]

Information Sharing Is Still a Source of Frequent Complaints

Industry partners consistently complain of the lack of effective, timely information and threat sharing from government partners despite consistent pledges from government to streamline the process and declassify information more rapidly. Industry stakeholders also complain that the federal government wants access to all their data without explaining why and that multiple agencies each separately request the same data. Even after government efforts to improve information sharing in the wake of the Russian invasion of Ukraine in February 2022, interviewees reported that their ability to access timely, useful information from the U.S. government has not substantially improved.

Yet even as the government has struggled to improve its performance, the information-sharing environment has been rapidly changing. In fact, the traditional concept of information sharing between the U.S. government and critical infrastructure — one that presupposes that the government has more or better data than the private sector — no longer accurately describes the relationship. In 2023, industry has a tremendous amount of insight and information about key elements of U.S. national security, particularly on cybersecurity issues, and in some cases — particularly domestically — outpaces the government's knowledge. Thus, any solutions to the information-sharing problem will need to work in both directions.

Efforts To Implement Resilience, Continuity, and Emergency Response Efforts Are Insufficient

Over the last several years, a consensus developed throughout the policy and cybersecurity communities that perimeter security alone is insufficient. Determined, well-resourced hackers can find ways to compromise all systems. Therefore, government and industry need a greater focus on resilience — that is, continuity of service through a crisis, coordination of emergency response, and the quick recovery of minimum viable functions. Despite this recognition, neither government nor industry has sufficiently prioritized resilience. In fact, there is little coordination between government programs that provide grants or other incentives for infrastructure security or resilience.

Meanwhile, over the past 15 years, the federal government has made many of its most significant investments in developing resilience infrastructure outside the SRMA framework or its cross-sector collaboration organizations.[96] A CISA resilience advisory subcommittee concluded in a September 2022 that more work is needed to promote resilience within the SRMA framework. The subcommittee noted that an "insufficient scope for national resiliency outcomes" hinders the improvement of national risk management.[97] It recommended creating "national resiliency goals to drive common analysis and action" and enhancing "enabling structures and programs to advance national resiliency goals.

Recommendations

Updating the national critical infrastructure protection framework is no small task. Doing so successfully requires both an understanding of the minutiae of individual SRMAs and their subcomponents as well as a holistic understanding of the SRMA framework. It requires a firm understanding of statute, policy, and practice, and it will require action and input by the executive branch, Congress, and industry alike.

Rewrite PPD-21 For a New Era

The Biden administration has already committed to rewriting PPD-21 and has begun a broad policy review in service of that goal, although questions remain about the scope and timeline of the planned revisions. A wholesale rewriting of PPD-21, however, risks undercutting those relationships, structures, and processes that have effectively promoted public-private collaboration.

The Biden administration can make the existing framework effective with targeted updates rather than starting from scratch. While revising the directive, the administration should communicate with stakeholders frequently and early in the drafting process. This dialogue should: 1) identify discrepancies or problems early on, 2) allow non-drafting stakeholders the time

to prepare for changes, and 3) model the collaborative partnership that the government says it wants. An open, transparent process would also likely ease consternation prompted by the idea of change. As a White House office statutorily tasked with coordinating and consulting with the private sector, the Office of the National Cyber Director should be a critical part of this process. The following recommendations outline what an updated PPD-21 should achieve.

1) Clearly identify strategic changes

PPD-21 communicates three strategic "imperatives" that merit preservation:

1. "Refine and clarify functional relationships across the federal government to advance the national unity of efforts to strengthen critical infrastructure security and resilience.
2. Enable effective information exchange by identifying baseline data and systems requirements for the federal government.
3. Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure."[98]

The rewrite of PPD-21 should add two strategic imperatives to focus more on resilience and continuity of operations (rather than focusing solely on security) and to recognize that stronger government oversight and regulation is needed to protect U.S. infrastructure. While this last point is controversial, the administration can find a path that addresses underperforming sectors while not burdening high-performing ones with new requirements.

2) Assign responsibilities and ensure accountability for routine updates of key strategic documents

A revised PPD-21 should ensure that the U.S. critical infrastructure protection framework receives updates via an iterative, repeatable process — rather than through a once-in-a-decade executive re-write or legislation when the executive branch fails to act.

There are several possible methods to ensure routine updates. One is to require that, every two years, administrations review strategic documents like PPD-21 and amend them accordingly. Another is to create a permanent process in DHS that enables strategic and policy updates without requiring a new presidential directive.

Either way, the Biden administration (and its successors) should ensure that PPD-21's successor never becomes as outdated as PPD-21 and that similar timeframes for reviewing, amending, and republishing the NIPP and SSPs are imposed.

The updated PPD-21 — or the NIPP — should also clarify what information SSPs should contain. SSPs should not be a box-checking exercise; if updated policy documents do not meet specified content standards, CISA must have the ability to send them back for revision, as discussed in the next section.

3) Clarify CISA's roles and responsibilities as NRMA

CISA's national risk management authorities stem from the Cybersecurity and Infrastructure Security Agency Act of 2018, which requires the director of CISA to "coordinate a national effort to secure and protect against critical infrastructure risks" consistent with the comprehensive National Infrastructure Protection Plan.[99] The replacement for PPD-21 should identify CISA as the NRMA and specify roles and responsibilities for CISA and its NRMC.

The update to PPD-21 should also, where necessary, increase or clarify CISA's ability to compel minimum security standards and to convene or require collaboration or engagement where appropriate. For example, the update should clarify which information SRMAs must collect and pass on to CISA for purposes of understanding national risk.

The update should also clarify expectations for CISA's own performance as the NRMA. For example, CISA needs to ensure the executive branch adheres to the timelines for review and revision of the NIPP and SSPs. CISA should also designate an executor agency for NIPP responsibilities — a standing entity that ensures there is always a cohesive body at CISA following through on NIPP requirements and holding other entities accountable for doing so.[100]

4) Resolve questions around the organization and designation of critical infrastructure sectors and assigned SRMAs

PPD-21's rewrite — or supporting guidance by the NRMA — should identify not just critical infrastructure sectors but also their subsectors. A new directive must articulate the process and timeline for adding, modifying, or removing sectors or subsectors and explain the guidelines for and value of subsector designations — or delegate this to the NRMA. DHS's Federal Senior Leadership Council would be the appropriate body to support and inform this organizational task.

The most obvious opportunities for adding and modifying sectors or subsectors are in space systems, communications, and cloud computing, where technologies and economic impact have changed dramatically over the past decade. The PPD-21 rewrite should also add a process for evaluating if the most suitable agencies are serving as SRMAs and for transferring responsibility if they are not.

5) Provide guidance on SRMA organization and operation

PPD-21's rewrite — or supporting guidance by the NRMA — should offer advice or directives for SRMAs on how to organize themselves and how to designate and document leadership roles and responsibilities. The rewrite should also offer SRMAs guidelines on conducting their tasking, including minimum baselines for performance. Given that some sectors are much stronger than others, there should be potential for grandfathering in existing structures that work. Ideally, PPD-21's successor will also resolve whether it is better to house a regulator and SRMA in the same entity, whether they should be separate, or whether different configurations are appropriate for different sectors.

The updated PPD-21 should also require federal agencies to publicly designate SRMA coordinators who report to the highest levels of the organization (deputy or cabinet secretary). These coordinators should be senior enough to testify to Congress, should have access to sufficient resources, and must be equipped to communicate directly with the hundreds or thousands of assets in their sector. If the administration does not make this update through a PPD-21 revision process, Congress should amend Section 9002 of the FY 2021 NDAA to establish these standards of seniority, access, and resources.

Finally, any discrepancies between PPD-21 tasking for SRMAs and FY 2021 NDAA tasking must be resolved. While the 9002(b) report argued that FY 2021 NDAA language is "aligned"[101] with PPD-21 tasking and merely makes explicit some additional "largely implicit" PPD-21 tasking, the GAO believes the legislation added new tasking.[102] It matters less which interpretation is correct and more that new documents are written clearly enough to avoid this type of confusion.

6) Facilitate accountability

PPD-21's rewrite — or supporting guidance by the NRMA — should clearly define roles, deadlines, and expectations not only for SRMAs but for state, local, tribal, and territorial governments and the private sector as well. This should include goals, assessments, timelines, and metrics for evaluating quantitatively how a sector is doing or how its SRMA is performing its own responsibilities, to ensure entities are held accountable under policy as well as law.

Support the PPD-21 Rewrite With Implementation and Resourcing Efforts

Many of the weaknesses of the current national critical infrastructure protection framework are ones of implementation. They will not be resolved with a PPD-21 rewrite. Thus, the White House and Congress will need to take the following steps to bolster the effectiveness of public-private collaboration.

7) Strengthen CISA's capabilities to execute its NRMA responsibilities

While PPD-21 should outline CISA's responsibilities, the agency itself must take the initiative to become the type of leader (as NRMA) that industry needs it to be. CISA is a young agency and has made great strides over the past several years, but it needs to become a true leader.

To begin with, CISA should prioritize developing more consistent organizational roles and responsibilities, as well as clear operational doctrine, for its NRMA role. If one expects CISA to uphold its complex responsibilities across multiple

administrations, it needs a strong fixed operational capability. CISA also must have the appropriate taskings to implement its authorities to update all policy documents and instruct SRMAs to update their SSPs.

Additionally, CISA should create and utilize a national risk register to identify, analyze, collate, and share information with interagency and industry partners more proactively. Cross-cutting entities, such as the Federal Senior Leadership Council, if strengthened, should provide a foundation to build out this effort. A more robust implementation of the NCFs will also support this. Notably, CISA's most recent strategic plan calls for the agency to "reinvigorate our role as the national authority on, and central repository of, the nation's critical infrastructure data" and to "mature CISA's risk analysis capabilities and methodologies"[103] — both of which indicate that CISA agrees at least in principle with this need.

Finally, setting up CISA to thrive may mean reviewing its responsibilities to ensure that it is not being asked to do too much. For example, in PPD-21, the secretary of homeland security is charged with executing critical infrastructure protection. In practice, however, this role has fallen very heavily upon CISA's director. While this may be appropriate in certain circumstances, the secretary can bring other agencies to bear and force action where CISA cannot. For example, the secretary could (and should) require that the National Advisory Council of the Federal Emergency Management Agency grant CISA a seat. For CISA to succeed, DHS senior leadership also needs to fulfill its infrastructure security roles, particularly in emergency response and physical infrastructure protection.

8) Resource SRMAs for the responsibilities they have

Effective SRMA organization and operations rely on adequate resourcing. The White House needs to ask for adequate funding and resourcing for SRMAs in annual budget requests and make the case to Congress that the SRMAs need these funds. Congress will then need to ensure that all SRMAs have sufficient authorities, resources, and processes. Each sector has unique regulators, ISACs, SCCs, GCCs, trade associations, and other stakeholders that are critical to the success of the public-private collaboration that SRMAs are meant to lead. Not all sectors need the same amount of support. Not all SRMAs need the same budgets. But all SRMAs should have sufficient resources to meet the needs of their sector.

Congress will also need to update statutes to ensure SRMAs have the necessary authorities to collaborate effectively and respond quickly to the needs of their sector. The White House's existing review of federal authorities should inform possible legislation. Congress will also need to exercise oversight to ensure SRMAs are properly fulfilling their obligations under the law.

9) Identify a more effective way to catalog, support, and protect priority infrastructure

Whether in PPD-21's successor or in a different document, the federal government needs a more effective process for working with industry to 1) designate SIEs (or SICI), 2) identify clear ways for the government to support these entities, and 3) require certain standards of performance from the private sector. All three elements are necessary.

The Biden administration has acknowledged the need to create an accurate list of SIEs, noting that its rewrite of PPD-21 would "provide clear guidance" to departments and agencies on "designating certain critical infrastructure as systemically important."[104] This is step one.

Step two requires that SIEs receive priority attention from the government — that is, they should receive something "useful" in exchange for their inclusion on this list. For example, SIEs could expect an improved delivery of actionable and timely cyber threat intelligence and joint cyber planning. Benefits could also include technical assistance in the form of government-provided continuous monitoring and detection of cyber risks and the regular exercise of response, recovery, and restoration plans. SIE/SICI entities could also gain liability protection against litigation following nation-state attacks, assuming the entity was meeting all government standards. Several of these — including the exploration of liability protections — would require congressional action.

At the same time, SIEs should face additional scrutiny concerning minimum standards for security and resiliency. This could include requirements that security measures be validated by third-party checks or resiliency tests or a requirement to have insurance. It may also include opportunities for DHS, CISA, SRMAs, or another entity to investigate certain of these "too-big-to-fail" entities to determine if there are dangerous chokepoints or dependencies and how to mitigate such problems.

10) Develop functional information-sharing capacity across all sectors

To address information-sharing gaps and the lack of a consensus view of the threat landscape, CISA, working with interagency partners (especially the National Security Agency), should establish a cyber threat information collaboration environment. This is a necessary complement to efforts to improve the SRMA framework. It will deepen operational collaboration between the government and the private sector by enhancing common situational awareness of cybersecurity threats and joint partnerships, including within the context of legislation on cyber incident reporting.

CISA has taken steps toward achieving shared situational awareness by leveraging its Joint Cyber Defense Collaborative for industry and government partners to improve cyber threat information sharing and collectively develop solutions. A collaborative data platform — with the technical means to enable the cross-correlation of information at the speed and scale necessary for rapid detection and identification of threats — is the next step in that maturation process. To that end, CISA proposed, in its FY 2024 budget request, merging existing programs into a data platform, called the Joint Collaborative Environment, for improved security monitoring.[105] Given this renewed CISA interest in a JCE, congressional action is required to fund this effort and include other data streams in the JCE (from the intelligence community, among others) to ensure it provides value to the private sector.

Congress should authorize the creation of a digital environment (or expand the mandate of CISA's effort) so that critical infrastructure participants can more quickly and effectively defend against cybersecurity threats to their networks. This digital environment should consist of technical tools for information analytics and a portal through which relevant government and industry parties can submit and access cyber threat information from different sources across the federal government — including the intelligence community — with the requisite clearances and permissions.

To address both industry and government concerns about data control, the environment should enable data owners to retain authority to set and maintain access controls, including to protect intelligence sources and methods. Congress should require the executive branch to establish procedures and data governance structures, as necessary, to protect data shared in the information collaboration environment; comply with federal regulations and statutes; and respect existing consent agreements with public and private sector critical infrastructure entities that apply to critical infrastructure information.

11) Organize public-private collaboration to mitigate systemic and cross-sector risk

The ability to understand and prioritize threats — within industries and sectors and across the whole ecosystem of critical infrastructure — is central to the success of the national critical infrastructure protection system. Nevertheless, the current understanding of systemic and cross-sector risk is immature.[106]

Both small-scale and systematic improvements should be made here. A smaller improvement would be that CISA and SRMAs can work to bolster their SCCs and GCCs so these bodies can better coordinate across sectors. Some sectors or subsectors are already including representatives on synergistic coordinating councils. More robust investment in the NCFs may also help build understanding of common risk. Focusing on critical functions helps shift analysis towards a greater understanding of risks to the delivery of services critical infrastructure provides rather than solely focusing on risks to particular companies or sectors.

12) Ensure effective emergency response

Multiple presidential directives and statutes direct emergency response. They date to the administrations of George W. Bush (HSPD-5) and Barack Obama (PPD-8, PPD-41, PPD-44) as well as the Stafford Act of 1988. The Biden administration should resolve the question, endemic in U.S. crisis response, of how private industry can coordinate with a single point of contact during an emergency and how the U.S. government can more appropriately coordinate among its components and respond. While a PPD-21 rewrite itself cannot rewrite other policy documents or other implementation documents, it should prompt a reevaluation and refinement of existing emergency response law and policy.

Conclusion

The codification of SRMAs into law, the ongoing drafting process for the NIPP, and the Biden administration's launch of a PPD-21 rewrite mean that more policymaker attention than usual is focused on the private-public partnerships that protect America's critical infrastructure. A unique window has opened in which policymakers can work together to revitalize and revamp the national critical infrastructure system and, particularly, the SRMA framework.

This will not require the wholesale gutting and replacement of existing partnerships, policies, and processes. Where there are beacons of success, the Biden administration and Congress should seek to preserve and build upon them. Where there are flaws, they must be addressed. After years of increasing nation-state and criminal cyber threats to U.S. national critical infrastructure — and in the face of renewed geopolitical tensions and additional stressors imposed by climate change — now is the time to update the critical infrastructure protection framework.

Appendix

No.	Sector (per PPD-21)	SRMA(s) (per PPD-21)	Delegated Agency or Office Leads (per 2015 Sector-Specific Plan)	Subsectors (per 2015 Sector-Specific Plan)	Subsectors (per CISA Website, Retrieved 2023)
1	Chemical sector	Department of Homeland Security	National Protection and Programs Directorate, Office of Infrastructure Protection	No subsectors listed (five "segments" specified: basic chemicals, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer products)	No subsectors listed (five "segments" specified: basic chemicals, specialty chemicals, agricultural chemicals, pharmaceuticals, and consumer products)
2	Commercial facilities sector	Department of Homeland Security	National Protection and Programs Directorate, Office of Infrastructure Protection	Entertainment/media	Entertainment/media
				Gaming	Gaming
				Lodging	Lodging
				Outdoor events	Outdoor events
				Public assembly	Public assembly
				Real estate	Real estate
				Retail	Retail
				Sports leagues	Sports leagues
3	Communications sector	Department of Homeland Security	National Protection and Programs Directorate, Office of Cybersecurity and Communications	No subsectors listed (five "component areas" specified: broadcast, cable, satellite, wireless, and wireline)	No subsectors listed
4	Critical manufacturing sector	Department of Homeland Security	National Protection and Programs Directorate, Office of Infrastructure Protection	No subsectors listed (four "component areas" specified: primary metals manufacturing; machinery manufacturing; electrical equipment, appliance, and component manufacturing; and transportation manufacturing)	No subsectors listed (four "component areas" specified: primary metals manufacturing; machinery manufacturing; electrical equipment, appliance, and component manufacturing; and transportation manufacturing)
5	Dams sector	Department of Homeland Security	National Protection and Programs Directorate, Office of Infrastructure Protection	One subsector listed: the levee subsector, which has its own coordinating council	No subsectors listed
6	Defense industrial base sector	Department of Defense	No 2015 SSP available	No subsectors listed (no 2015 plan has been made public; however, the 2010 plan offers nine "industry segments:" aircraft; ships; tracked and wheeled land vehicles; electronics; soldier systems; structural; munitions; space; and mechanical)	No subsectors listed

No.	Sector (per PPD-21)	SRMA(s) (per PPD-21)	Delegated Agency or Office Leads (per 2015 Sector-Specific Plan)	Subsectors (per 2015 Sector-Specific Plan)	Subsectors (per CISA Website, Retrieved 2023)
7	Emergency services sector	Department of Homeland Security	National Protection and Programs Directorate, Office of Infrastructure Protection	No subsectors listed (five "distinct disciplines" specified: law enforcement; fire and rescue services; emergency medical services; emergency management; and public works)	No subsectors listed (five "distinct disciplines" specified: law enforcement; fire and rescue services; emergency medical services; emergency management; and public works)
8	Energy sector	Department of Energy	Unspecified in Energy's 2015 SSP; however, today the role is executed via the Office of Cybersecurity, Energy Security, and Emergency Response	Electricity Oil and gas	No subsectors listed (three "interrelated segments" are specified: electricity, oil, and natural gas)
9	Financial Services sector	Department of the Treasury	Treasury's Office of Critical Infrastructure and Compliance Policy	No subsector listed (four "service categories" specified: deposit, consumer credit, and payment systems products; credit and liquidity products; investment products; and risk transfer products, including insurance)	No subsectors listed
10	Food and agriculture sector	Department of Agriculture and Department of Health and Human Services	Health and Human Services: The Food and Drug Administration's Office of Analytics and Outreach/Food Defense and Emergency Coordination Staff at the Center for Food Safety and Applied Nutrition (per 2013 NIPP, Health and Human Services is SSA — now SRMA — for food that is not meat, poultry, or processed egg products*) Department of Agriculture: Leadership for SSA responsibilities rests with the Office of Homeland Security and Emergency Coordination (per 2013 NIPP, Agriculture is SSA — now SRMA — for agriculture and meat, poultry, and processed egg products*)	No subsectors listed (a detailed taxonomy of the sector is provided, and a "beverage subsector" is referenced, but there is no list enumerating subsectors)	No subsectors listed

No.	Sector (per PPD-21)	SRMA(s) (per PPD-21)	Delegated Agency or Office Leads (per 2015 Sector-Specific Plan)	Subsectors (per 2015 Sector-Specific Plan)	Subsectors (per CISA Website, Retrieved 2023)
11	Government facilities sector	Department of Homeland Security and General Services Administration	The General Services Administration and the Department of Homeland Security's Federal Protective Service are the co-SSAs. The Department of Education's Office of Safe and Drug-Free Schools serves as the SSA for the education facilities subsector. The Department of the Interior serves as the SSA for the national monuments and icons subsector. The Department of Homeland Security serves as the SSA for the election subsector (per a 2020 subsector-specific annex).	Education facilities	Education facilities
				National monuments and icons	National monuments and icons
					Election infrastructure
12	Healthcare and public health sector	Department of Health and Human Services	Office of the Assistant Secretary for Preparedness and Response's Critical Infrastructure Protection Program Office	Direct patient care	No subsectors listed
				Health information technology	
				Health plans and payers	
				Mass fatality management services	
				Medical materials	
				Laboratories, blood, and pharmaceuticals	
				Public health	
				Federal response and program offices	
13	Information technology sector	Department of Homeland Security	National Protection and Programs Directorate, Office of Cybersecurity and Communications	No subsectors listed (six "critical functions" specified: provide IT products and services; provide incident management capabilities; provide domain name resolution services; provide identity management and associated trust support services; provide internet-based content, information, and communications services; and provide internet routing, access, and connection services)	No subsectors listed

No.	Sector (per PPD-21)	SRMA(s) (per PPD-21)	Delegated Agency or Office Leads (per 2015 Sector-Specific Plan)	Subsectors (per 2015 Sector-Specific Plan)	Subsectors (per CISA Website, Retrieved 2023)
14	Nuclear reactors, materials, and waste sector	Department of Homeland Security	National Protection and Programs Directorate, Office of Infrastructure Protection	Commercial nuclear power*	No subsectors listed
				Fuel cycle facilities	
				Research, training, and test reactor (RTTR) or research and test reactor (RTR)**	
15	Transportation systems sector	Department of Homeland Security and Department of Transportation	Department of Homeland Security: Transportation Security Administration and U.S. Coast Guard Department of Transportation: Office of Intelligence, Security, and Emergency Response	Aviation	Aviation
				Maritime	Highway and motor carrier
				Surface transportation	Maritime transportation system
				Postal and shipping	Mass transit and passenger rail
					Pipeline systems
					Freight rail
					Postal and shipping
16	Water and wastewater systems sector	Environmental Protection Agency	Unspecified in the 2015 SSP	No subsectors listed (two types of "infrastructure" are identified: drinking water and wastewater)	No subsectors listed
Sources	https://www.cisa.gov/sector-risk-management-agencies	https://www.cisa.gov/sector-risk-management-agencies	Individual 2015 Plans	Individual 2015 Plans	https://www.cisa.gov/sector-risk-management-agencies
			*Red text indicates office no longer exists. These sectors now look to CISA as their SRMA, a role it fulfills through the newly created Stakeholder Engagement Division	*The 2015 Nuclear Reactors, Materials, and Waste Sector-Specific Plan references several subsectors but does not list them comprehensively. Accordingly, this list may be incomplete.	
				**The 2015 Nuclear Reactors, Materials, and Waste Sector-Specific Plan references the research and test reactor subsector but lists the category above as including "researcher, training, and test reactor." It also references a nuclear SCC radioisotopes sub-council but does not say whether this is a subsector.	

Endnotes

1. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, §9002(c), 116th Congress (2021). (https://www.congress.gov/bill/116th-congress/house-bill/6395)

2. Tim Starks, "The Biden National Cyber Strategy is Unlike Any Before It," *The Washington Post,* January 6, 2023. (https://www.washingtonpost.com/politics/2023/01/06/biden-national-cyber-strategy-is-unlike-any-before-it)

3. See, for example, CISA Cybersecurity Advisory Committee, "Report to the CISA Director: Building Resilience and Reducing Systemic Risk to Critical Infrastructure," September 13, 2022. (https://www.cisa.gov/sites/default/files/publications/CSAC_SR_September_2022_Final_Recommendations_09132022-508.pdf)

4. The White House, "National Cybersecurity Strategy," March 2023. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

5. U.S. Executive Order 13010, "Critical Infrastructure Protection," July 15, 1996. (https://irp.fas.org/offdocs/eo13010.htm)

6. The White House, "Presidential Decision Directive/NSC-63," May 22, 1998. (https://irp.fas.org/offdocs/pdd/pdd-63.htm); U.S. Office of Homeland Security, "National Strategy for Homeland Security," July 2002. (https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf)

7. The White House, "Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience," February 12, 2013. (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

8. The election infrastructure is often thought of as a 17th sector, but in reality, DHS made it a subset of the government facilities sector in January 2017.

9. U.S. Department of Homeland Security, "National Infrastructure Protection Plan 2009," 2009. (https://www.cisa.gov/publication/nipp-2009-partnering-enhance-protection-resiliency)

10. U.S. Department of Homeland Security, "NIPP 2013: Partnering for Critical Infrastructure Security and Resilience," 2013. (https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf); Cybersecurity and Infrastructure Security Agency, "2015 Sector-Specific Plans," accessed December 3, 2022. (https://www.cisa.gov/2015-sector-specific-plans)

11. There are two exceptions to this generalization. The 2015 SSP from the Department of Defense (the lead agency for the Defense Industrial Base) remains "pending" on CISA's website, and the Healthcare and Public Health Sector published its SSP in 2016.

12. U.S. Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013. (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity)

13. U.S. Department of Homeland Security, "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience," 2013. (https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf)

14. Cybersecurity and Infrastructure Security Agency, "Support to Critical Infrastructure at Greatest Risk ('Section 9 Report') Summary," May 8, 2018. (https://www.cisa.gov/publication/support-critical-infrastructure-greatest-risk-section-9-report-summary)

15. Of note, EO 13636 excepted information technology providers from consideration as Section 9 entities: "The Secretary shall not identify any commercial information technology products or consumer information technology services under this section."

16. The White House, "Presidential Policy Directive/PPD-8: National Preparedness," March 30, 2011. (https://www.dhs.gov/xlibrary/assets/presidential-policy-directive-8-national-preparedness.pdf)

17. The White House, "Presidential Policy Directive/PPD-41: United States Cyber Incident Coordination," July 26, 2016. (https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident).

18. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, §9002(c), 116th Congress (2021). (https://www.congress.gov/bill/116th-congress/house-bill/6395)

19. Ibid.

20. Cybersecurity and Infrastructure Security Agency, "FY 2021 National Defense Authorization Act Section 9002(b) Report," November 12, 2021. (https://www.cisa.gov/sites/default/files/publications/Section_9002_NDAA_Report_FINAL_508c.pdf)

21. Sara Friedman, "Biden Administration Launches Plan to Review Relationship Between CISA and Sector Risk Management Agencies," *Inside Cybersecurity,* November 11, 2022. (https://insidecybersecurity.com/daily-news/biden-administration-launches-plan-review-relationship-between-cisa-and-sector-risk)

22. The White House, "Letter from the President to Select Congressional Leadership on the Nation's Critical Infrastructure," November 7, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/07/letter-from-the-president-to-select-congressional-leadership-on-the-nations-critical-infrastructure)

23. Joseph A. Blount, Jr., "Testimony of Joseph Blount, President and Chief Executive Officer Colonial Pipeline Company," *Hearing before the U.S. Senate Homeland Security and Governmental Affairs Committee*, June 8, 2021. (https://www.hsgac.senate.gov/hearings/threats-to-critical-infrastructure-examining-the-colonial-pipeline-cyber-attack)

24. Author analysis augmented by author interview with former CISA leadership.

25. Samantha Schwartz, "CISA Left in the Dark During Colonial Pipeline's Initial Response," *Cybersecurity Dive,* May 12, 2021. (https://www.cybersecuritydive.com/news/colonial-pipeline-ransomware-cisa-senate-hearing/600029)

26. Ibid.

27. U.S. Government Accountability Office, "Our Testimony to Congress on Efforts to Secure Oil and Gas Pipelines Against Cyberattacks," July 28, 2021. (https://www.gao.gov/blog/our-testimony-congress-efforts-secure-oil-and-gas-pipelines-against-cyberattacks-video)

28. "Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack," *Joint Hearing before the House Homeland Security Subcommittees on Cybersecurity, Infrastructure Protection, and Innovation and on Transportation and Maritime Security*. June 15, 2015. (https://www.govinfo.gov/content/pkg/CHRG-117hhrg45310/pdf/CHRG-117hhrg45310.pdf)

29. U.S. Government Accountability Office, "Our Testimony to Congress on Efforts to Secure Oil and Gas Pipelines Against Cyberattacks," July 28, 2021. (https://www.gao.gov/blog/our-testimony-congress-efforts-secure-oil-and-gas-pipelines-against-cyberattacks-video)

30. "Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack," *Joint Hearing before the House Homeland Security Subcommittees on Cybersecurity, Infrastructure Protection, and Innovation and on Transportation and Maritime Security,* June 15, 2021. (https://www.govinfo.gov/content/pkg/CHRG-117hhrg45310/pdf/CHRG-117hhrg45310.pdf)

31. U.S. Department of Homeland Security, "DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators," May 27, 2021. (https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators)

32. Aaron Schaffer and Ellen Nakashima, "New Emergency Cyber Regulations Lay Out 'Urgently Needed' Rules for Pipelines But Draw Mixed Reviews," *The Washington Post,* October 3, 2021. (https://www.washingtonpost.com/national-security/cybersecurity-energy-pipelines-ransomware/2021/10/03/6df9cab2-2157-11ec-8200-5e3fd4c49f5e_story.html)

33. Charlie Mitchell, "American Gas Association Weighs in on TSA Cybersecurity Proposal Covering Pipelines and Rail," *Inside Cybersecurity,* December 1, 2022. (https://insidecybersecurity.com/daily-news/american-gas-association-weighs-tsa-cybersecurity-proposal-covering-pipelines-and-rail)

34. Author interviews with industry and government experts.

35. The White House, "Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience," February 12, 2013. (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil); For more information, see also: U.S. Department of Homeland Security and U.S. Department of Energy, "Energy Sector-Specific Plan," 2015. (https://www.cisa.gov/sites/default/files/publications/nipp-ssp-energy-2015-508.pdf)

36. Cybersecurity and Infrastructure Security Agency, "Energy Sector Government Coordinating Council Charter," updated November 2019. (https://www.cisa.gov/sites/default/files/publications/Energy%20Sector%20GCC%20Charter%20Updated%20November%202019-508.pdf)

37. Nihal Krishan, "Big Boosts to Cybersecurity and Tech Funding in $1.7T Omnibus Bill Signed by Biden," *FedScoop*, December 30, 2022. (https://www.fedscoop.com/big-boosts-to-cybersecurity-and-tech-funding-in-1-7t-omnibus-bill-signed-by-biden)

38. Federal Energy Regulatory Commission, "FERC Adopts FAST Act Provisions on Critical Infrastructure Information," November 17, 2016, (https://www.ferc.gov/news-events/news/ferc-adopts-fast-act-provisions-critical-infrastructure-information)

39. Cybersecurity and Infrastructure Security Agency, "Electricity Sub-Sector Coordinating Council Charter," approved August 5, 2013. (https://www.cisa.gov/sites/default/files/publications/Energy-Electricity-SCC-Charter-2013-508.pdf)

40. Author interviews with industry experts.

41. "Cybersecurity Risk Information Sharing Partnership," *E-ISAC,* accessed March 1, 2023. (https://www.eisac.com/s/crisp)

42. "Industry Membership," *ONG-ISAC*, accessed December 1, 2022, (https://ongisac.org/membership/industry-membership)

43. "About the E-ISAC," Electricity Information Sharing and Analysis Center, accessed December 1, 2022. (https://www.eisac.com/s/about-the-eisac)

44. U.S. Coast Guard, "United States Coast Guard Cyber Strategic Outlook," August 2021, pages 5 and 12. (https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf)

45. Author interview with transportation sector experts.

46. Ibid.

47. "Transportation Safety Regulation in the United States Government," U.S. Department of Transportation, updated April 15, 2016. (https://www.transportation.gov/office-policy/transportation-policy/transportation-safety-regulation-united-states-government)

48. Sonya T. Proctor, "Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack," *Written Testimony before the Committee on Homeland Security Subcommittee on Transportation and Maritime Security,* June 15, 2021. (https://www.congress.gov/117/meeting/house/112775/witnesses/HHRG-117-HM08-Wstate-ProctorS-20210615.pdf)

49. U.S. Government Accountability Office, "Critical Infrastructure Protection: Actions Needed to Address Significant Weaknesses in TSA's Pipeline Security Program Management," December 19, 2018. (https://www.gao.gov/products/gao-19-48); U.S. Government Accountability Office, "Critical Infrastructure Protection: Key Pipeline Security Documents Need to Reflect Current Operating Environment," June 5, 2019, (https://www.gao.gov/products/gao-19-426)

50. U.S. Department of Homeland Security and U.S. Department of Transportation, "Transportation Systems Sector Activities Progress Report," 2018. (https://www.cisa.gov/sites/default/files/publications/transportation_systems_sector_activities_progress_report_20190503_508.pdf)

51. Aaron Schaffer, "Railroads Say They Don't Need Cybersecurity Mandates," *The Washington Post,* October 7, 2021. (https://www.washingtonpost.com/politics/2021/10/07/railroads-say-they-dont-need-cybersecurity-mandates); Chris Riotta, "TSA Administrator Says New Cyber Requirements in the Works for Aviation Industry," *Federal Computer Week*, November 18, 2022. (https://fcw.com/security/2022/11/tsa-administrator-says-new-cyber-requirements-works-aviation-industry/379901)

52. Author interview with industry and transportation sector experts. Interviewees were split on whether this funding is sufficient.

53. U.S. Department of Homeland Security and U.S. Environmental Protection Agency, "2015 Water and Wastewater Sector Specific Plan," June 2015. (https://www.cisa.gov/sites/default/files/publications/nipp-ssp-water-2015-508.pdf)

54. Mark Montgomery and Trevor Logan, "Poor Cybersecurity Makes Water a Weak Link in Critical Infrastructure," *Foundation for Defense of Democracies*, November 18, 2021. (https://www.fdd.org/analysis/2021/11/18/poor-cybersecurity-makes-water-a-weak-link-in-critical-infrastructure)

55. Three programs (Natural Disasters and Defense Preparedness, Water Security Initiative, and Cybersecurity) shared a budget of $10.3 million last year. See: U.S. Environmental Protection Agency, "United States Environmental Protection Agency Fiscal Year 2022 Justification of Appropriation Estimates for the Committee on Appropriations, Tab 03: Science and Technology," May 2021. (https://www.epa.gov/system/files/documents/2021-07/fy22-cj-03-science-technology.pdf)

56. Christian Vasquez, "EPA issues water cybersecurity mandates, concerning industry and experts," *CyberScoop*, March 3, 2023. (https://cyberscoop.com/epa-water-cyber-regulations)

57. Chris Riotta, "EPA Seeks Funding to Improve the Cybersecurity of America's Water Systems," *Federal Computer Weekly*, May 20, 2022. (https://fcw.com/security/2022/05/epa-pushes-improve-cybersecurity-americas-water-systems/367214); John Sakellariadis, "Russia's Cyber Offensive in 2023," *Politico*, December 21, 2022. (https://subscriber.politicopro.com/newsletter/2022/12/russias-cyber-offensive-in-2023-00074905)

58. U.S. Government Accountability Office, "Critical Infrastructure Protection: CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector," November 2021. (https://www.gao.gov/assets/720/717685.pdf); U.S. Government Accountability Office, "CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing," March 2022. (https://www.gao.gov/assets/gao-22-104279.pdf)

59. U.S. Government Accountability Office, "Critical Infrastructure Protection: Education Should Take Additional Steps to Help Protect K-12 Schools from Cyber Threats," October 2021. (https://www.gao.gov/assets/720/717088.pdf)

60. U.S. Government Accountability Office, "Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges," March 2021. (https://www.gao.gov/assets/gao-21-288.pdf)

61. U.S. Department of Homeland Security, "National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience," 2013, page 25. (https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf)

62. U.S. Government Accountability Office, "Critical Infrastructure Protection: Education Should Take Additional Steps to Help Protect K-12 Schools from Cyber Threats," October 2021. (https://www.gao.gov/assets/720/717088.pdf)

63. Author interview with former CISA leadership.

64. U.S. Department of Homeland Security, "Joint National Priorities for Critical Infrastructure Security and Resilience," September 28, 2018. (https://www.cisa.gov/sites/default/files/publications/Joint-National-Priorities-Fact-Sheet-20180928-508.pdf)

65. For example, CISA's reference page divides the energy sector into "three interrelated segments," while the 2015 energy SSP refers to itself as having "two sub-sectors." The nuclear sector's 2015 SSP references several subsectors in the text but does not list them comprehensively. The transportation sector's 2015 SSP lists four subsectors, but CISA's reference page mentions seven, and industry representatives say there are seven.

66. Frank Cilluffo, Mark Montgomery, Sharon Cardash, and Kelsey Shields, "Time to Designate Space Systems as Critical Infrastructure," *CSC 2.0*, April 14, 2023. (https://cybersolarium.org/csc-2-0-reports/time-to-designate-space-systems-as-critical-infrastructure)

67. U.S. Government Accountability Office, "CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector," November 2021. (https://www.gao.gov/assets/720/717685.pdf)

68. Author interview with former CISA leadership.

69. U.S. Government Accountability Office, "CISA Should Assess the Effectiveness of its Actions to Support the Communications Sector," November 2021, page 31. (https://www.gao.gov/assets/720/717685.pdf)

70. Tim Starks, "The Biden National Cyber Strategy is Unlike Any Before It," *The Washington Post*, January 6, 2023. (https://www.washingtonpost.com/politics/2023/01/06/biden-national-cyber-strategy-is-unlike-any-before-it)

71. U.S. Department of Homeland Security, "Chemical Sector-Specific Plan: An Annex to the NIPP 2013," 2015, pages 19-20. (https://www.cisa.gov/sites/default/files/publications/nipp-ssp-chemical-2015-508.pdf)

72. Cybersecurity and Infrastructure Security Agency, "CISA Strategy Plan: 2023-2025," September 2022, (https://www.cisa.gov/sites/default/files/publications/StrategicPlan_20220912-V2_508c.pdf). Notably, however, the NRMC does not currently have an explicit leadership role in the SRMA framework.

73. Cybersecurity and Infrastructure Security Agency, "CISA Strategy Plan: 2023-2025," September 2022, (https://www.cisa.gov/sites/default/files/publications/StrategicPlan_20220912-V2_508c.pdf)

74. Author interviews.

75. U.S. Government Accountability Office, "CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing," March 1, 2022. (https://www.gao.gov/assets/gao-22-104279.pdf)

76. Author interview with former CISA leadership.

77. For example, in testimony on April 6, 2022, Eric Goldstein, CISA's executive assistant director for cybersecurity, explained to Congress that CISA does not have the ability to compel organizations to share cybersecurity information. This makes it difficult to assess risk overall. See: "Mobilizing our Cyber Defenses: Maturing Public-Private Partnerships to Secure U.S. Critical Infrastructure," *Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation of the Committee on Homeland Security, House of Representatives,* April 6, 2022. (https://www.congress.gov/event/117th-congress/house-event/LC68630/text?s=1&r=48)

78. Cyberspace Solarium Commission, "Cyberspace Solarium Commission Final Report," March 2020, page 55. (https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf)

79. Cybersecurity and Infrastructure Security Agency, "FY 2021 National Defense Authorization Act Section 9002(b) Report," November 12, 2021, page 5. (https://www.cisa.gov/sites/default/files/publications/Section_9002_NDAA_Report_FINAL_508c.pdf)

80. The White House, "National Cybersecurity Strategy," March 2023. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

81. The White House, "National Cybersecurity Strategy," March 2023, page 8. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf). According to the 2023 "National Cybersecurity Strategy," "While voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, the lack of mandatory requirements has resulted in inadequate and inconsistent outcomes."

82. Cyberspace Solarium Commission, "Cyberspace Solarium Commission Final Report," March 2020, page 56. (https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf)

83. CISA Cybersecurity Advisory Committee, "Report to the CISA Director: Building Resilience and Reducing Systemic Risk to Critical Infrastructure," September 13, 2022. (https://www.cisa.gov/sites/default/files/publications/CSAC_SR_September_2022_Final_Recommendations_09132022-508.pdf)

84. Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Cross Sector Council Charter," approved November 12, 2015. (https://www.cisa.gov/sites/default/files/publications/cipac-cross-sector-council-charter-2015-508.pdf)

85. Cybersecurity and Infrastructure Security Agency, "Federal Senior Leadership Council Charter," renewed March 15, 2021. (https://www.cisa.gov/sites/default/files/publications/fslc-charter-2021-508.pdf)

86. "National Critical Functions," Cybersecurity and Infrastructure Security Agency, accessed December 1, 2022. (https://www.cisa.gov/national-critical-functions)

87. U.S. Department of Homeland Security and Cybersecurity and Infrastructure Security Agency, "Election Infrastructure Subsector-Specific Plan: An Annex to the NIPP 2013," 2020. (https://www.cisa.gov/sites/default/files/publications/election_infrastructure_subsector_specific_plan.pdf)

88. Interview with former CISA leadership.

89. Cybersecurity and Infrastructure Security Agency, "FY 2021 National Defense Authorization Act: Section 9002(b) Report," November 12, 2021, page 35. (https://www.cisa.gov/sites/default/files/2023-01/Section_9002_NDAA_Report_FINAL_508c.pdf). The Section 9002(b) report calls for "a periodic evaluation to confirm or modify the SRMA-sector alignment [that] should take into account the statutorily defined SRMA roles and responsibilities, the requirements associated with the corresponding sector, and the authorities and capabilities of the department or agency in question in order to optimally align SRMA designations." However, it does not itself outline how to accomplish this task.

90. The White House, "National Cybersecurity Strategy," March 2023, page 8. (https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf)

91. U.S. Government Accountability Office, "CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing," March 1, 2022, page 48. (https://www.gao.gov/assets/gao-22-104279.pdf)

92. CISA Cybersecurity Advisory Committee, "Report to the CISA Director: Building Resilience and Reducing Systemic Risk to Critical Infrastructure," September 13, 2022. (https://www.cisa.gov/sites/default/files/publications/CSAC_SR_September_2022_Final_Recommendations_09132022-508.pdf)

93. Cyberspace Solarium Commission, "Cyberspace Solarium Commission Final Report," March 2020, page 97. (https://cybersolarium.org/wp-content/uploads/2022/05/CSC-Final-Report.pdf)

94. CISA Cybersecurity Advisory Committee, "Report to the CISA Director: Building Resilience and Reducing Systemic Risk to Critical Infrastructure," September 13, 2022. (https://www.cisa.gov/sites/default/files/publications/CSAC_SR_September_2022_Final_Recommendations_09132022-508.pdf)

95. Cybersecurity and Infrastructure Security Agency, "FY 2021 National Defense Authorization Act Section 9002(b) Report," November 12, 2021. (https://www.cisa.gov/sites/default/files/publications/Section_9002_NDAA_Report_FINAL_508c.pdf)

96. Peer review feedback from former government officials, February 16, 2023, and February 22, 2023. Some of the most significant investments include the American Recovery and Reinvestment Act of 2009, the Building Resilient Infrastructure and Communities program of the Federal Emergency Management Agency, the Inflation Reduction Act, and other disaster recovery funds and opportunity zones.

97. CISA Cybersecurity Advisory Committee, "Report to the CISA Director: Building Resilience and Reducing Systemic Risk to Critical Infrastructure," September 13, 2022. (https://www.cisa.gov/sites/default/files/publications/CSAC_SR_September_2022_Final_Recommendations_09132022-508.pdf)

98. The White House, "Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience," February 12, 2013. (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

99. Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. 115-278, 132 Stat. 4168. (https://www.congress.gov/115/plaws/publ278/PLAW-115publ278.pdf)

100. An obvious example would be the requirement in the NIPP to update SSPs every four years.

101. Cybersecurity and Infrastructure Security Agency, "FY 2021 National Defense Authorization Act Section 9002(b) Report," November 12, 2021. (https://www.cisa.gov/sites/default/files/publications/Section_9002_NDAA_Report_FINAL_508c.pdf)

102. U.S. Government Accountability Office, "Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities," February 2023. (https://www.gao.gov/assets/gao-23-105806.pdf). According to this GAO report, "GAO found that the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 expanded and added responsibilities for sector risk management agencies."

103. Cybersecurity and Infrastructure Security Agency, "CISA Strategic Plan 20223-2025," September 2022. (https://www.cisa.gov/sites/default/files/publications/StrategicPlan_20220912-V2_508c.pdf)

104. The White House, "Letter from the President to Select Congressional Leadership on the Nation's Critical Infrastructure," November 7, 2022. (https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/07/letter-from-the-president-to-select-congressional-leadership-on-the-nations-critical-infrastructure)

105. U.S. Department of Homeland Security, "Department of Homeland Security: Cybersecurity and Infrastructure Security Agency Budget Overview," March 2023. (https://www.dhs.gov/sites/default/files/2023-03/CYBERSECURITY%20AND%20INFRASTRUCTURE%20SECURITY%20AGENCY.pdf)

106. This is why, in the report of the CISA resilience advisory subcommittee, it recommended that greater efforts be undertaken at this time to understand systemic risk within NCFs at a high level, rather than focusing on sub-issues or cross-sector risks.

About the Authors

Mary Brooks is a public policy fellow at the Wilson Center, focusing on cybersecurity and technology. She was previously a Fellow in the Cybersecurity and Emerging Threats program at the R Street Institute, an associate producer for HBO documentaries "Year One" and "The Perfect Weapon," and a special assistant at the public interest law firm, Perseus Strategies. Her work has been published by the Aspen Strategy Group, Lawfare, *The National Interest*, and *The Hill*, among others.

Annie Fixler is the director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies and an FDD research fellow. She works on issues related to cyber-enabled economic warfare, the national security implications of cyberattacks on economic targets, adversarial strategies and capabilities, and U.S. cyber resilience. She also contributes to the work of FDD's Transformative Cyber Innovation Lab and Center on Economic and Financial Power.

RADM (Ret.) Mark Montgomery is the senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. He also directs CSC 2.0, having served as the Cyberspace Solarium Commission's executive director. Previously, Mark served as policy director for the Senate Armed Services Committee, coordinating policy efforts on national security strategy, capabilities and requirements, and cyber policy. Mark served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017.

ACKNOWLEDGEMENTS

The authors would like to thank the many government and industry experts who agreed to be interviewed for this report and offered unparalleled insights and constructive feedback during the research and writing process. This report would be a shadow of itself without their honest assessments and thoughtful analysis. While many experts helped refine the conclusions, any errors in fact or judgment are ours alone. We are also grateful to David Adesnik, Miriam Himmelfarb, and David May for their eagle-eyed edits and to Daniel Ackerman and Erin Blumenthal for the design and production of this report.

Cover Photo: Workers stand on scaffolding on a residential building under construction. (Photo by Sean Gallup/Getty Images)

About CSC 2.0

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission (CSC). Congress created the CSC in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The commission operated successfully for two and a half years, publishing its flagship report in March 2020 along with subsequent white papers. The CSC issued more than 80 recommendations to reform U.S. government structures and organization, strengthen norms and non-military tools, promote national resilience, reshape the cyber ecosystem, operationalize public-private collaboration, and preserve and employ military instruments of national power.

At the CSC's planned sunset, the commissioners launched the CSC 2.0 project to support continued efforts to implement outstanding CSC recommendations, provide annual assessments of the implementation of CSC recommendations, and conduct research and analysis on several outstanding cybersecurity issues identified during the commission's tenure.

For more information, visit **www.CyberSolarium.org**.

Co-Chairmen

Angus S. King Jr., U.S. Senator for Maine

Michael "Mike" J. Gallagher, U.S. Representative for Wisconsin's 8th District

Distinguished Advisors

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Thomas A. "Tom" Fanning, Chairman, President, and Chief Executive Officer of Southern Company

Chris Inglis, Former U.S. National Cyber Director

James R. "Jim" Langevin, Former U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

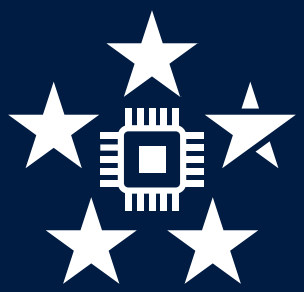
Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Benjamin E. "Ben" Sasse, Former U.S. Senator for Nebraska

Suzanne E. Spaulding, Senior Adviser for Homeland Security at the Center for Strategic and International Studies

Partners

FDD



CSC 2.0

Preserving and Continuing the Cyberspace Solarium Commission