FY 2021 National Defense Authorization Act

Section 9002(b) Report

November 12, 2021

Cybersecurity and Infrastructure Security Agency

This page intentionally left blank

FY2021 NATIONAL DEFENSE AUTHORIZATION ACT: SECTION 9002(b) REPORT

TABLE OF CONTENTS

1. Executive Summary

Our national infrastructure security is built on a partnership between government and private industry that combines the implementation of policy, regulatory, and voluntary actions to manage risk. Both public and private entities own and operate the Nation's critical infrastructure, but the risk associated with the destruction or failure of that infrastructure is borne by a much larger population of Americans—and disproportionately by vulnerable or disadvantaged communities, and people of color. For this reason, the effort to secure the Nation's critical infrastructure requires a whole-of-government approach and coordination and collaboration across multiple intergovernmental and industry stakeholders. The Cybersecurity and Infrastructure Security Agency (CISA) Act of 2018, as codified in 6 U.S.C. § 652(c)(4), requires the Director of CISA to "coordinate a national effort to secure and protect against critical infrastructure risks" consistent with a comprehensive national plan (currently the National Infrastructure Protection Plan 2013, hereafter referred to as the National Plan) required in (e)(1)(E) of the same subchapter.

This existing national infrastructure security framework provides a collaborative partnership model for consolidating information and expertise from government and industry. Working with critical infrastructure sectors, the Federal Government ensures the security and resilience of the Nation's infrastructure through the use of tools and resources like bi-directional threat information sharing, real-world exercises, incident response training and guidance, federally-led risk assessments and analysis, and subject matter expertise. Active engagement with public- and private-sector partners inform this national framework and its associated tools and resources, which those partners rely on for the security of their systems and assets.

As detailed in this report, the current framework for securing the Nation's critical infrastructure originated from presidential policy decisions in the 1990s and subsequent provisions in the 2000s that recognized both the expanding scale of terrorism and other threats, and the emerging cybersecurity challenge of increasingly networked and internet-enabled infrastructure systems. The Federal Government has an opportunity to evaluate and enhance the current approach to accommodate updates to national policy; leverage lessons learned from the operation of the national partnership through steady state activities, real-world events, and exercises; and consider new and evolving national security threats and cybersecurity risks.

On behalf of the Department of Homeland Security (DHS), CISA is providing this report as required under Sec. 9002 of the 2021 National Defense Authorization Act (NDAA) which codified Sector-Specific Agencies (SSAs), previously defined in Presidential Policy Directive 21 (PPD-21), as Sector Risk Management Agencies (SRMAs), and defined how DHS and SRMAs should work

with each other to protect critical infrastructure.[1] Within 180 days, the NDAA required the Secretary of Homeland Security, in consultation with the heads of SRMAs, to review the current framework for securing critical infrastructure, as outlined in the National Plan, developed pursuant to 6 U.S.C. § 652(e)(1)(E). As required by Section 9002(b) of the 2021 NDAA, the Secretary was also required to evaluate the current list of critical infrastructure sectors and current designations for SRMAs, and provide recommendations for revisions to the President.

This report describes the resulting assessment and findings and outlines several recommendations for consideration. As required, this report recommends a process and structure for identifying and designating sectors and aligning those sectors to designated SRMAs. The findings highlight an opportunity to designate a Space Sector and Bioeconomy Sector, depending on a review process described in further detail below. CISA will collaborate with each SRMA to evaluate the list of sectors and SRMAs through a phased approach to validate and refine the activities of the current sector structure.

Some of the recommendations described below may change depending upon the implementation of new uniform statutory authorities, roles, and responsibilities for SRMAs contained in Section 9002(c), which now appear in the U.S. Code at 6 U.S.C. § 665d. Future periodic reviews can more completely assess SRMA and sector performance in line with these new authorities and roles.

1.1. Method

CISA led the evaluation effort required by Sec. 9002(b) of the 2021 NDAA, establishing a collaborative approach for this consultation with SRMAs and other federal interagency partners. CISA conducted facilitated discussion sessions with federal interagency partners leveraging regular "SRMA Coordination Calls" during March, April, and May 2021, increasing the frequency of those calls during the review period. CISA also consulted with SRMAs through the Federal Risk Management Working Group chartered under the Federal Senior Leadership Council (FSLC). The evaluation effort was informed by recommendations from the CISA COVID-19 Task Force, which reviewed the draft report.

SRMA consultations were managed in two parts: (1) facilitated discussions, and (2) data calls using an online unstructured data collection platform. CISA leveraged this online collaboration platform to elicit input and feedback from interagency partners.

The main areas of focus for the facilitated discussions included:

- validating the criteria to define/identify a critical infrastructure sector;
- defining SRMA roles and responsibilities and introducing capabilities and common

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

baseline activities as organizing structure; and

- introducing criteria to inform Government Coordinating Council (GCC) membership.

The following factors shaped the overall scope and extent of this analysis.

- The review was conducted within the 180-day time constraint of the fiscal year (FY) 2021 NDAA.
- The review of the current framework was constrained to assessing the existing mechanisms, authorities, policies, and function of the overall partnership. In short, the review focused on the National Plan required pursuant to 6 U.S.C. § 652(e)(1)(E).
- The cross-sector working group supporting the initial refresh of the National Plan (established under the auspices of the Critical Infrastructure Partnership Advisory Council [CIPAC]) included representation from SRMAs, Information Sharing and Analysis Centers and Organizations, academia, and other agencies.
- The Sec. 9002(b) consultation was focused on existing SRMAs.

1.2. Findings and Recommendations

CISA's evaluation led to the identification of several findings and a set of recommendations for consideration. The following table summarizes the result of this effort.

Findings	Recommendations
Finding 1. CISA can improve national governance by maturing its role as the National Coordinator of activities to secure and protect against critical infrastructure risks under 6 U.S.C. § 652(c)(4) and clarifying, in collaboration with SRMAs, the processes to modify sector and SRMA designations and assess sector maturity and remain nimble and adaptable to changing risks in support of this role.	CISA, in collaboration with the Office of the National Cyber Director (ONCD) the National Security Council (NSC), and Sector Risk Management Agencies (SRMAs) should clarify federal roles and responsibilities for sector risk management and sector coordination, build processes to support its responsibilities as National Coordinator, and lead the implementation of the recommendations in this report, as appropriate.
	CISA and the SRMAs should leverage the Federal Senior Leadership Council (FSLC) to develop a process for modifying the sector structure and/or the corresponding SRMA designations.
	The FSLC should serve as an interagency consensus decision-making body with oversight and governance responsibilities for the national effort.
	CISA should lead an FSLC Working Group to validate and implement the processes outlined in Appendices C and D of this report.
	The FSLC should develop, and SRMAs should implement, a customizable methodology for each SRMA to assess the maturity and effectiveness of their sector-specific partnership structures.
Finding 2. The Federal Government can improve coordination and implementation of the national effort to secure the Nation's infrastructure by updating existing national and sector- specific plans, establishing risk management priorities for each sector, and providing guidance and resources to SRMAs to perform roles and responsibilities.	CISA, in collaboration with ONCD, NSC, and the SRMAs, with input from other relevant departments and agencies, should update the National Plan, including clarifying the role of the National Critical Functions (NCF) in establishing risk management priorities across sectors.
	CISA, in collaboration with ONCD, NSC, and SRMAs, and with input from other relevant departments and agencies, should apply the framework outlined in this report to evaluate the scope of current critical infrastructure sectors to ensure they appropriately address systems, assets, National Critical Functions, and capabilities; evaluate potential modifications to SRMA designations; and evaluate the potential establishment of new sectors or subsectors.

Findings	Recommendations
	CISA should lead an effort through the FSLC to identify both cross-sector and individual sector risk management priorities and requirements.
	CISA should lead an effort to expand and strengthen cross-sector coordination structures to address rapidly evolving or urgent risks.
Finding 3. SRMAs require greater consistency in resources and doctrine, which would reinforce SRMA operations, enable the development of clearer objectives and performance goals, and improve coordination with other key Federal agencies and partners.	CISA should collaborate with SRMAs to improve processes and tools for carrying out their responsibilities in a manner that avoids duplication with services provided centrally by CISA.
	CISA should lead an effort through the FSLC to develop a baseline SRMA cost estimation tool to assist in budget formulation and to provide recommendations to the Office of Management and Budget (OMB) on the implementation of a consistent resource request process to support execution of SRMA responsibilities.
	All SRMAs, coordinating through the FSLC, should develop sector-specific implementation plans outlining specific authorities and capabilities, objectives, priorities, as well as a four-year roadmap outlining key activities to be implemented in carrying out the responsibilities under Section 2215 of the Homeland Security Act of 2002.
	CISA should establish a National Coordinator SRMA assistance model, providing resources for enhanced coordination and technical support for sector-level risk analysis to SRMAs.
Finding 4. Voluntary coordination and partnerships are vital for information sharing and collaboration. However, a coordinated national effort to secure the nation's infrastructure can do more to directly inform, encourage, and coordinate risk reduction actions.	CISA, in coordination with the FSLC, should explore ways to incentivize and jointly develop and implement security and risk mitigation actions through the national partnership, incorporating and reflecting the risk reduction benefits of adherence to standards, best practices, and regulatory requirements.
	CISA, in collaboration with ONCD, and NSC other relevant departments and agencies, should conduct a review of risk management collaboration mechanisms and/or to incentivize implementation of security and risk mitigation actions.
Finding 5. There is a need for stronger risk assessment, vulnerabilities analysis, information sharing, coordination mechanisms, and actionable countermeasures to manage cross-sector risks and incidents.	The FSLC should establish a working group to develop a National Infrastructure Assessment, Analysis, and Data Framework as a supplement to the National Plan.
	The FSLC should establish a working group to develop a National Infrastructure Intelligence Sharing Framework as a supplement to the National Plan.

Findings	Recommendations
	The FSLC should establish a working group to develop a National Infrastructure Incident Coordination Framework as a supplement to the National Plan.

2. INTRODUCTION

2.1. Background

Critical infrastructure supports the national and economic security of the United States, as well as the provision of vital services and performance of essential functions. The disruption, unavailability, or destruction of that infrastructure could have debilitating national effects, driving the shared national interest in a strong federal capacity to secure critical infrastructure.

Both public- and private-sector entities own and operate the Nation's critical infrastructure, with the risk associated with the destruction or failure of that infrastructure borne by a much larger population—disproportionately by disadvantaged communities and people of color. There are varying types of risk and not all infrastructure is subject to the same risk. For example, societal risk can reflect a host of social inequalities and disproportionately affect vulnerable populations.

Exchanging information between public- and private-sector entities requires an effective multi-stakeholder collaboration model that protects critical infrastructure information and consolidates expertise from government and industry. Protection of critical infrastructure is governed by voluntary standards, regulatory requirements, and, in many cases, voluntary best practices. These factors should necessitate the prioritization of federal resources against cross-sector risk and risks faced by each critical infrastructure sector, and requires a national approach that recognizes the value of both voluntary coordination, and the application of consensus standards, regulatory tools, and incentives to drive risk reduction.

The Nation's health, safety, and economy depend on an increasingly complex, interconnected set of infrastructure systems facing multiple stressors and rapidly changing threats and demands. Protecting America's critical infrastructure is neither an exclusively public or private interest; it is a shared multi-level and multi-jurisdictional challenge with often overlapping responsibilities, requiring a collaborative enterprise that can ensure the resilience of infrastructure while ensuring the life, health, and safety of all Americans and allowing the economy it supports to grow, innovate, and prosper.

Sec. 9002(c) of the 2021 NDAA codified SSAs (previously defined in PPD-21) as SRMAs and defined how DHS and SRMAs work with each other to protect critical infrastructure. Within 180 days, the Secretary of Homeland Security, in consultation with the heads of SRMAs, was required to review the current framework for securing critical infrastructure (as outlined in the corresponding National Plan), evaluate the current list of critical infrastructure sectors and current designations for SRMAs, and provide recommendations for revisions to the President.

CISA managed the evaluation effort required by Sec. 9002(b) of the 2021 NDAA, establishing a collaborative approach for this consultation with SRMAs and other federal interagency partners. This report describes the resulting assessment, identifies several findings, and outlines

recommendations for consideration.

2.2. Purpose

This report addresses the requirement established by Sec. 9002(b) of the 2021 NDAA, which directed the Secretary of Homeland Security, in consultation with the heads of the SRMAs, to evaluate the current framework to secure the Nation's infrastructure and submit to the President and appropriate congressional committees a report that includes information about how DHS assessed the current framework to secure the Nation's infrastructure, the list of designated critical infrastructure sectors and subsectors, and the designated SRMAs, as follows:

(b) **CRITICAL INFRASTRUCTURE SECTOR DESIGNATION.**—

(1) INITIAL REVIEW.—Not later than 180 days after the date of the enactment of this section, the Secretary, in consultation with the heads of Sector Risk Management Agencies, shall—

(A) review the current framework for securing critical infrastructure, as described in section 2202(c)(4) of the Homeland Security Act (6 U.S.C. 652(c)(4)) and Presidential Policy Directive 21; and

(B) submit to the President and appropriate congressional committees a report that includes—

(i) information relating to—

(I) the analysis framework or methodology used to—

(aa) evaluate the current framework for securing critical infrastructure referred to in subparagraph (A); and

(bb) develop recommendations to—

(AA) revise the current list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, any successor or related document, or policy; or

(BB) identify and designate any subsectors of such sectors; and

(II) the data, metrics, and other information used to develop the recommendations required under clause (ii); and

(ii) recommendations relating to—

(I) revising—

(aa) the current framework for securing critical infrastructure referred to in subparagraph (A);

(bb) the current list of critical infrastructure sectors designated pursuant to Presidential Policy Directive 21, any successor or related document, or policy; or

(cc) the identification and designation of any subsectors of such sectors; and

(II) any revisions to the list of designated Federal departments or agencies that serve as the Sector Risk Management Agency for a sector or subsector of such section, necessary to comply with paragraph (3)(B).

2.3. Scope

This initial review applies to current designated SRMAs and critical infrastructure sectors, to the current policy and National Plan frameworks in place pursuant to 6 U.S.C. § 652, PPD-21, and to

other relevant active policies and executive orders.

2.4. Approach

CISA conducted initial planning and research during January and February 2021, while concurrently finishing the first draft of the National Plan refresh, which was distributed for comment in February 2021. Facilitated discussion sessions with SRMAs and other federal interagency partners leveraged regular coordination calls during March, April, and May of the same year, which were conducted on a bi-weekly basis. In addition, CISA leveraged an online unstructured data collection platform to collect additional input from interagency partners.

3. ASSESSMENT OF CURRENT STATE

3.1. Overview

DHS has the responsibility to coordinate a national effort to secure and protect against critical infrastructure risks and to develop a comprehensive national plan for securing critical infrastructure under the Homeland Security Act of 2002. Pursuant to applicable authority, the Secretary of Homeland Security delegated this overall responsibility to CISA.

3.2. Cybersecurity and Infrastructure Security Agency

CISA is responsible for coordinating a national effort to secure the Nation's critical infrastructure.[2] CISA is the operational component of DHS that leads this infrastructure security and resilience mission for the department.

CISA provides a variety of cyber and infrastructure security capabilities and services to non-federal organizations, including assessments and analysis, capacity building, expertise and guidance, and security operations (e.g., incident response and threat hunting). CISA's cybersecurity and infrastructure security missions seek to drive improved security and resilience, as well as to minimize the prevalence and impact of cybersecurity and physical incidents across critical infrastructure. Both aspects of CISA's mission are dependent on partnerships with the critical infrastructure community.

CISA has a unique role within the ecosystem of sectors and SRMAs—serving as an SRMA (see: section 3.3.4), the National Coordinator (see: section 3.3.3), and a centralized provider of risk reduction services across sectors. In this last role, CISA maintains unique authorities, resources, and capabilities to build upon sectoral expertise present in each SRMA to understand risk and take active steps to protect the Nation's critical infrastructure.

The following table summarizes the capabilities and services provided under CISA's specialized authorities. The table is organized according to five baseline capabilities that are essential for executing responsibilities associated with the National Coordinator role (cross-sector responsibilities), as well as the responsibilities associated with the SRMA role (sector-specific responsibilities).

[2] 6 U.S.C. § 652 outlines the CISA Director's roles and responsibilities.

Table 1: CISA's Capabilities and Services Relevant to SRMA Responsibilities

Baseline Capability	CISA's Capabilities and Services
Partnership Management	• Coordinate the national effort to secure the Nation's critical infrastructure. • Coordinate national cyber asset response activities in concert with the Federal Government and industry representatives as appropriate. • Oversee a national ecosystem of government and sector coordinating councils, forums, and collaboration mechanisms.
Planning, Analysis, and Reporting	• Lead the development and periodic updates of the National Plan. • Partner with SRMAs in understanding how all-hazards risks could disrupt sector operations. • Conduct cross-sector analysis to identify dependencies and potential cascading effects to disruptions to National Critical Functions that could result from cyber intrusions, other man-made threats, or natural hazards affecting the Nation's critical infrastructure. • Conduct cross-sector analysis to identify and prioritize linkages between National Critical Functions and sector systems, assets, and networks; and to identify and prioritize risk management activities. • Help critical infrastructure entities identify cybersecurity intrusions and threats by offering CISA-provided tools or querying commercial detection and sensing deployed by critical infrastructure entities. • Coordinate with additional Federal frameworks.
Capacity Building	• Develop national guidance, standards, and best practices to enhance the security and resilience of the Nation's critical infrastructure. • Provide cybersecurity capabilities that help critical infrastructure entities identify and reduce cybersecurity risks, such as vulnerability scanning, penetration testing, and architecture reviews. • Improve the security and resilience capabilities of critical infrastructure entities through technical assistance, facility-specific or regional-level assessments (addressing cyber, physical, and cyber-physical aspects), training programs, and exercise services.
Information Sharing	• Produce and disseminate actionable threat intelligence, alerts, warnings, and guidance to help critical infrastructure organizations understand and mitigate emerging risks. • Maintain a national database of critical infrastructure. • Collect, protect, and share sensitive information and analysis with sector entities.
Incident Management	• Coordinate cross-sector operations among critical infrastructure entities, businesses, and government partners to stabilize community lifelines and impacted National Critical Functions during an incident through Emergency Support Function (ESF) #14. • Provide incident response and threat hunting services to critical infrastructure entities potentially impacted by cybersecurity intrusions. • Support federal disaster recovery and mitigation operations through the National Preparedness System • Work with federal partners to provide technical guidance on homeland security grant programs.

3.3. Coordinating a National Effort

3.3.1. Critical Infrastructure

Within the current national policy framework provided by PPD-21, "the term 'critical infrastructure' has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42

U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[3]

Critical infrastructure sectors, as defined in the National Plan, are a logical collection of assets, systems, or networks that provide common functions to the economy, government, or society.[4] Sectors are not distinctions of different types of risk but are defined in and recognized through doctrinal changes to the partnership structure and associated collaboration mechanisms defined by the National Plan and designed to facilitate the coordination of risk management activities for the Nation's critical infrastructure. Infrastructure that meets the definition of criticality defined in 42 U.S.C. 5195c(e) is organized and addressed through the National Plan partnership framework and the sector coordination model.

The statutorily required National Plan [pursuant to 6 U.S.C. § 652(e)(1)(E) and 6 U.S.C. §652(c)(4)] addresses 16 critical infrastructure sectors, as identified in PPD-21. DHS and other designated federal departments and agencies organize and execute many vital missions according to the sector structure. This includes the statutory responsibility to coordinate with interagency and industry partners through the sector structure, to facilitate cross-sector coordination to address cybersecurity risks and incidents. Sectors within the partnership structure established by the National Plan are often broken down into subsectors that address specific logical subgroups or risk challenges within a given sector.

3.3.2. The National Plan

The Homeland Security Act, as amended and codified in 6 U.S.C. § 652, requires DHS, through CISA, to produce a comprehensive national plan to secure the Nation's critical infrastructure and key resources. This plan describes how the United States secures its infrastructure through a national partnership for managing risk.

The requirements for a national plan for securing the Nation's key resources and critical infrastructure originates in the Homeland Security Act of 2002. Different versions of the National Plan were published in 2005 (interim), 2006, 2009, and most recently in 2013. The Homeland Security Act and each of the subsequent iterations of this plan reinforced the criticality of a strong public-private partnership to collectively identify and develop structures, processes, programs, and

---

[3] White House, *Presidential Policy Directive (PPD) 21, Critical Infrastructure Security and Resilience* (Washington, DC: White House, February 12, 2013).

[4] Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, DC: DHS, 2013) https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

resources that improve the security posture of the Nation's critical infrastructure.

The National Plan was last updated in 2013 when PPD-21: *Critical Infrastructure Security and Resilience* directed key improvements to the National Plan, including:

- a risk management framework for security and resilience;
- methods to be used to prioritize critical infrastructure;
- protocols to be used to synchronize communication and actions within the Federal Government; and
- metrics and analysis process to be used to measure the Nation's ability to manage and reduce risks to critical infrastructure.

PPD-21 also required the 2013 National Plan to reflect the identified functional relationships within DHS and across the Federal Government and the updates to the public-private partnership model, to consider sector dependencies on energy and communications systems, and to identify pre-event and mitigation measures or alternate capabilities during disruptions to those systems.

The 2013 National Plan served as the national plan for securing the Nation's infrastructure for the last eight years and continues to do so until the update is completed. Numerous changes in the policy and operating environments for critical infrastructure, as well as a complex and rapidly changing risk environment have created the need for an updated National Plan.

3.3.3. The National Coordinator

The CISA Act of 2018, as codified in 6 U.S.C. §652(c)(4), requires the Director of the Agency to "coordinate a national effort to secure and protect against critical infrastructure risks" consistent with the National Plan required in (e)(1)(E) of the same subchapter. This responsibility to coordinate a national effort requires CISA to organize, lead, and execute across a federal ecosystem that includes federal agencies with designated responsibilities as SRMAs, as well as a broader national effort that brings together state, local, tribal, territorial, and private sector partners.

CISA also carries out responsibilities pursuant to PPD-21. As delegated by the Secretary of Homeland Security, the Director of CISA is the designated National Coordinator for the critical infrastructure security and resilience. The national approach for securing critical infrastructure has always included the figure of a National Coordinator who is responsible for coordinating the actions of other federal agencies. Prior to the creation of DHS, this responsibility fell to the Executive Office of the President. The 1998 Presidential Decision Directive 63 (PDD-63) established multiple responsibilities for this National Coordinator role, including interagency coordination for policy development and implementation and advice regarding agency budgets for critical infrastructure protection.

The Homeland Security Act of 2002 placed on DHS the responsibility to coordinate a national effort to secure and protect against critical infrastructure risks and to develop a comprehensive

national plan for securing critical infrastructure. The 2003 Homeland Security Presidential Directive 7 (HSPD-7) described the role of DHS in coordinating overall efforts to enhance the protection of the Nation's critical infrastructure, including the establishment of policies, approaches, guidelines, and methodologies for integrating federal infrastructure protection and risk management activities within and across sectors. PPD-21 further defined the role of DHS in coordinating the national effort to promote the security and resilience of critical infrastructure. With the creation of CISA in 2018, the responsibility for the development of a national plan for securing critical infrastructure was assigned to its director.

To shape and complement that work, CISA will work closely with the Executive Office of the President, specifically the Office of the National Cyber Director (ONCD) and the National Security Council (NSC), to develop a broad vision for the implementation and operationalization of national cybersecurity and infrastructure priorities. CISA will work with the National Cyber Director (NCD)[5] and the Homeland Security Advisor to ensure that CISA's central role as the National Coordinator is reinforced and advanced. SRMAs will further mature capabilities, where needed, to provide unique sectoral expertise in risk management, partnership development, and emergency preparedness, as prescribed in the FY2021 NDAA.

The National Coordinator role gives CISA the responsibility to establish processes for coordinating cybersecurity and infrastructure security actions across SRMAs and the Federal Government, and for collaboration between government and industry to share information or jointly respond to cybersecurity or other threats or incidents. DHS operates with specialized statutory authority for convening and sharing information with private sector entities, and as National Coordinator, the Director of CISA is responsible for ensuring a unified approach to risk management that addresses the full spectrum of risks to critical infrastructure. CISA is charged with coordinating directly with private sector partners, safeguarding Protected Critical Infrastructure Information (PCII), and establishing and managing public-private collaboration mechanisms. While CISA has a unique responsibility for ensuring that such coordination occurs within a unified national effort, individual agencies with authority, expertise, and capability within a given sector have responsibilities as SRMAs, which are described in the next section. In addition, as described above, CISA provides a variety of services and capabilities to help critical infrastructure organizations understand, manage, and reduce risk. These capabilities can be deployed and adapted most effectively when combined with unique sectoral expertise from SRMAs.

3.3.4. Sector Risk Management Agencies

The term "Sector Risk Management Agency" (SRMA) refers to a federal department or agency,

[5] The NCD is intended to play a critical role in working with federal departments and agencies on developing and implementing policies and strategies to make the NSC's strategic vision a reality.

designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.[6] The definition of SRMA is mirrored in PPD-21 under the term "sector-specific agency (SSA)."[7] The FY2021 NDAA modified the Homeland Security Act to codify SSAs as SRMAs, and replaced all statutory references to SSAs with references to SRMAs.[8]

6 U.S.C. § 655 describes SRMA responsibilities in detail. In implementing their responsibilities, SRMAs are required by law to coordinate with DHS and other federal agencies; to collaborate with critical infrastructure owners and operators within their sectors; and to coordinate with state, local, tribal and territorial partners within their sector. Carrying out SRMA responsibilities requires extensive coordination with the Director of CISA. SRMAs are required by law to coordinate with the Director of CISA in prioritizing and performing vulnerability assessments; risk assessments; intelligence and information sharing activities; critical infrastructure information data sharing; incident response and preparedness activities; and a range of other SRMA functions. This places a special responsibility on the Director of CISA to establish the means and mechanisms to support that coordination, to define national approaches for how SRMAs conduct this work, and to ensure that CISA provides centralized capabilities that effectively support critical infrastructure entities in coordination with SRMAs.

Most SRMAs updated their respective Sector-Specific Plans (SSPs) following the publication of the National Plan in 2013. Those SSPs currently serve as the strategic documents organizing sector activity and priorities in support of the Joint National Priorities for critical infrastructure security and resilience. SSPs are unique to each sector and vary in their level of description about particular sector activities, or the approach the sector will take in organizing and applying the available tools for partnership and information sharing. The National Plan includes "calls to action" but does not direct sector-specific priorities or initiatives.[9]

The 2013 National Plan recognizes existing regulatory authorities inherent in SRMAs, and also recognizes that critical infrastructure may be regulated by state, local, tribal, and territorial (SLTT)

---

[6] 6 U.S.C. § 651(5)

[7] Office of the Press Secretary, The White House, "Presidential Policy Directive—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] U.S. Congress, House, *William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021*, Sec. 9002. Sector Risk Management Agencies, H.R. 6395, 116th Congress, January 1, 2021, https://www.congress.gov/bill/116th-congress/house-bill/6395.

[9] Cybersecurity and Infrastructure Security Agency, "2015 Sector-Specific Plans," accessed July 2, 2021, https://www.cisa.gov/2015-sector-specific-plans.

governments, though the current version of the plan does not further define or describe the operational integration of regulatory mechanisms and approaches into the national partnership approach. SRMAs are designated for their respective sectors based on authorities and capabilities specific to that sector. PPD-21 recognizes that "Each critical infrastructure sector has unique characteristics, operating models, and risk profiles that benefit from an identified SSA that has institutional knowledge and specialized expertise about the sector." PPD-21 also defines the roles and responsibilitiesto be carried out by all SRMAs in recognition of the existing statutory or regulatory authorities of federal departments and agencies and existing sector familiarity and relationships. Section 9002 of the FY2021 NDAA subsequently amended the Homeland Security Act to codify SRMA roles and responsibilities. SRMA performance will be regularly audited by the U.S. Government Accountability Office (GAO) pursuant to the modification to the Homeland Security Act, however, additional guidance may be helpful to assist SRMAs in identifying human resource and budgetary needs for fulfilling SRMA roles and responsibilities.

3.4. Categorization of Critical Infrastructure Sectors

The National Plan defines sectors as "a logical collection of assets, systems, or networks that provide a common function to the economy, government, or society."[10] Executive Order (EO) 13010 (1996) describes specific sectors as "critical infrastructure," specifically identifying telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government as "vital" national "critical infrastructures." The Clinton Administration later established a more extensive federal regime for critical infrastructure security in PDD-63 (1998), which established 12 critical infrastructure sectors and "special functions" and assigned lead agencies to each.

[10]Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (Washington, DC: DHS, 2013) https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

Table 2: PDD-63 Sectors and Special Functions and Lead Agencies

PDD-63 Sectors and Special Functions		PDD-63 Lead Agencies
Sectors	Information and Communications	Department of Commerce
	Banking and Finance	Department of the Treasury
	Water Supply	Environmental Protection Agency
	Aviation, Highways, Mass Transit, Pipelines, Rail Waterborne Commerce	Department of Transportation
	Emergency Law Enforcement Services	Department of Justice
	Emergency Fire Service	Federal Emergency Management Agency
	Continuity of Government Services	Federal Emergency Management Agency
	Public Health Services	Department of Health & Human Services
	Electric Power	Department of Energy
	Oil and Gas Production and Storage	Department of Energy
Functions	Law Enforcement and Internal Security	Department of Justice
	Foreign Intelligence	Central Intelligence Agency
	Foreign Affairs	Department of State
	National Defense	Department of Defense

Two executive orders that predated the establishment of DHS addressed critical infrastructure protection—EO 13228 and EO 13231, both in 2001. They made no changes to the lead agency designations under PDD-63, but they referred to additional critical infrastructure sectors not identified in PDD-63, including nuclear facilities, food and agriculture, and manufacturing.

The first major changes to critical infrastructure sector and lead agency designations came in the *National Strategy for Homeland Security* (2002), released when the creation of DHS had been proposed but not yet enacted.

Table 3: Critical Infrastructure Sectors and Lead Agencies under the National Strategy for Homeland Security (2002)

Sectors under 2002 Homeland Security Strategy	Lead Agencies
Agriculture	Department of Agriculture
Food: Meat and Poultry	Department of Agriculture
Food: All other products	Department of Health & Human Services
Water	Environmental Protection Agency
Public Health	Department of Health & Human Services
Emergency Services	Department of Homeland Security
Government: Continuity of Government	Department of Homeland Security
Government: Continuity of Operations	All Departments and Agencies
Defense Industrial Base	Department of Defense
Information and Telecommunications	Department of Homeland Security
Energy	Department of Energy
Transportation	Department of Homeland Security (in coordination with Department of Transportation)
Banking and Finance	Department of the Treasury
Chemical Industry and Hazardous Materials	Environmental Protection Agency
Postal and Shipping	Department of Homeland Security
National Monuments and Icons	Department of the Interior

The *National Strategy for Homeland Security* broadened the range of critical infrastructure sectors while also dropping the federal "special functions" identified in PDD-63. It emphasized unity of effort and consolidation of critical infrastructure responsibilities under DHS.[11] In addition to being given responsibility for coordinating the overall national critical infrastructure protection effort, DHS was assigned as lead agency for five out of the 14 critical infrastructure sectors. These sectors included some that were analogous to sectors under PDD-63, such as Information and Telecommunications (previously assigned to the Department of Commerce [DoC]) and Transportation (previously assigned to the Department of Transportation [DoT]).

The *National Strategy for Physical Protection of Critical Infrastructure* in 2003 made incremental changes to the sector structure, creating a new category of "key assets" (later called key resources)

[11] "Our country requires a single accountable official to ensure we address vulnerabilities that involve more than one infrastructure sector or require action by more than one agency. Our country also requires a single accountable official to assess threats and vulnerabilities comprehensively across all infrastructure sectors to ensure we reduce the overall risk to our country, instead of inadvertently shifting risk from one potential set of targets to another. Under the President's proposal, the Department of Homeland Security will assume responsibility for integrating and coordinating federal infrastructure protection responsibilities." *National Strategy for Homeland Security* (2002), p. 31.

distinct from critical infrastructure sectors.[12] Those assets included nuclear power plants (under the lead of the Nuclear Regulatory Commission in coordination with DHS), dams (DHS lead), national monuments and icons (Interior lead), government facilities (co-lead with DHS and the General Services Administration [GSA]), and commercial key assets (DHS lead). This strategy made no changes to the critical infrastructure sectors (aside from re-designating national monuments and icons as key assets) or to the lead agencies for those sectors.

In 2003, HSPD-7 was released, which reformulated critical infrastructure sector lead agencies as SSAs. The sector designations remained largely the same, except that DHS was named the SSA for the Chemical Sector in place of the Environmental Protection Agency (EPA), as well as the lead SSA for the Government Facilities Sector instead of its previous co-lead role. The first National Plan (2006) developed the SSA concept further and reiterated the SSA assignments, including identifying responsibilities at the DHS component level. DHS was also given a more explicit leading SSA role for the Commercial Nuclear Reactors, Material, and Waste Sector while continuing to work with the U.S. Nuclear Regulatory Commission (NRC).[13] Additionally, the Education Facilities Subsector within Government Facilities Sector was established with the Department of Education identified as the corresponding SSA.

In 2008, the Secretary of Homeland Security made the first use of the authority under HSPD-7 to designate a new sector, Critical Manufacturing. DHS was named the SSA for this new sector. In 2009, the Obama administration issued an updated National Plan (2009), which kept the previous administration's sector structure intact.

More extensive changes arrived with the issuance of PPD-21 and a new version of the National Plan (2013). The distinction between critical infrastructure sectors and key resources was dropped. National Monuments and Icons became a subsector under Government Facilities, and Postal and Shipping a subsector under Transportation Systems. DHS's role as SSA for the Government Facilities and Transportation Systems Sectors became a co-lead role alongside GSA and Department of Transportation, respectively.

The sector structure outlined by PPD-21 and the 2013 version of the National Plan remains in place today. The only change to the sector structure between 2013 and the enactment of the 2021 NDAA took place in 2017 with the designation of Election Infrastructure as a subsector of the

---

[12] Key assets were "individual targets whose destruction could cause large-scale injury, death, or destruction of property, and/or profoundly damage our national prestige, and confidence." *National Strategy for Physical Protection of Critical Infrastructure* (2003), p. 7.

[13] The NRC licenses and regulates the Nation's civilian use of radioactive materials to provide reasonable assurance of adequate protection of public health and safety, to promote the common defense and security, and to protect the environment. Consistent with this mission, the NRC has promulgated robust safety and security regulations applicable to certain critical infrastructure entities subject to the NRC's jurisdiction within the Nuclear Reactors, Materials, and Waste Sector.

Government Facilities Sector.

Table 4: Current Critical Infrastructure Sector Structure

Current Sectors	Current SRMAs
Chemical	Department of Homeland Security
Commercial Facilities	Department of Homeland Security
Communications	Department of Homeland Security
Critical Manufacturing	Department of Homeland Security
Dams	Department of Homeland Security
Emergency Services	Department of Homeland Security
Information Technology	Department of Homeland Security
Nuclear Reactors, Materials, and Waste	Department of Homeland Security
Food and Agriculture	Department of Agriculture Department of Health & Human Services
Defense Industrial Base	Department of Defense
Energy	Department of Energy
Healthcare and Public Health	Department of Health & Human Services
Financial Services	Department of the Treasury
Water and Wastewater Systems	Environmental Protection Agency
Government Facilities	Department of Homeland Security, General Services Administration
Transportation Systems	Department of Homeland Security, Department of Transportation

In summary, the Federal Government has changed what it considers to be critical infrastructure sectors at least 12 times since 1996.[14] At least six of those changes also involved revisions to the assignments of lead roles for federal agencies for certain critical infrastructure sectors. The revisions vary widely in scope and purpose and reflect the vast changes in the threat landscape and in the Federal Government's structure since the 1990s.

When DHS was created in 2002, there were 14 critical infrastructure sectors. Since then, the Federal Government has added four new sectors and removed two, subsuming them into other sectors. Table 5 shows the evolution of the sector structure since 1998, as well as DHS's responsibilities as a lead or lead agency to coordinate across the sectors. The table shows that the relative proportion of critical infrastructure categories under the responsibility of DHS has continuously increased over the years, from 36 percent since the establishment of the Department

[14] EO 13010 (1996), PDD-63 (1998), EO 13228 (2001), EO 13231 (2001), National Strategy for Homeland Security (2002), National Strategy for Physical Protection of Critical Infrastructure (2003), HSPD-7 (2003), National Infrastructure Protection Plan (2006), addition of the Critical Manufacturing Sector (2008), National Infrastructure Protection Plan (2009), PPD-21 and National Infrastructure Protection Plan 2013, addition of Election Infrastructure Subsector (2017).

to 63 percent currently.

Table 5: Evolution of the Critical Infrastructure Sector Structure since 1998

Critical Infrastructure Sector or Key Asset/Resource [15]	PDD-63 (1998)	NSHS (2002)	NSPPCI (2003)	HSPD-7 (2003)	N.I.P.P. (2006)	N.I.P.P. (2009)	PPD-21 (2013) N.I.P.P. (2013)
Chemical / Chemical Industry & Hazardous Materials	-	EPA	EPA	DHS	DHS	DHS	DHS
Commercial Facilities	-	-	DHS	DHS	DHS	DHS	DHS
Communications / Telecommunications	DoC	DHS	DHS	DHS	DHS	DHS	DHS
Critical Manufacturing	-	-	-	-	-	DHS	DHS
Dams	-	-	DHS	DHS	DHS	DHS	DHS
Defense Industrial Base	-	DoD	DoD	DoD	DoD	DoD	DoD
Emergency Services / Emergency Fire Services	FEMA	DHS	DHS	DHS	DHS	DHS	DHS
Energy	DoE	DoE	DoE	DoE	DoE	DoE	DoE
Government Facilities / Government Services	FEMA	DHS	DHS GSA	DHS	DHS	DHS	DHS GSA
Healthcare and Public Health	HHS	HHS	HHS	HHS	HHS	HHS	HHS
Information Technology	DoC	DHS	DHS	DHS	DHS	DHS	DHS
Financial Services / Banking and Finance	Treas.	Treas.	Treas.	Treas.	Treas.	Treas.	Treas.
Food and Agriculture	-	USDA HHS	USDA HHS	USDA HHS	USDA HHS	USDA HHS	USDA HHS
National Monuments and Icons	-	-	DoI	DoI	DoI	DoI	-
Nuclear Reactors, Materials, and Waste	-	-	NRC DHS	NRC DHS	DHS[16]	DHS	DHS
Postal and Shipping	-	DHS	DHS	DHS	DHS	DHS	-
Transportation Systems	DoT	DHS	DHS	DHS	DHS	DHS	DHS DoT
Water and Wastewater Systems / Water Supply	EPA	EPA	EPA	EPA	EPA	EPA	EPA

[15] The names of the sectors and key assets or resources in the first column of Table 5 are the current or most recent names. Some sectors have been split or combined at various points. Consequently, the numbers in the "DHS (Lead or Co-Lead)" row may not match the number of times "DHS" appears in the columns above. The "DHS Total" numbers reflect the actual numbers of sectors in existence at the time and under the doctrine indicated in the top row, as well as the actual number of sectors for which DHS was designated as the lead agency at the time.

[16] In National Infrastructure Protection Plan (2006), DHS was given a more explicit leading role for the Nuclear Reactors, Materials, and Waste Sector while continuing to work with the NRC, which is responsible for licensing and regulating the Nation's civilian use of radioactive materials.

Critical Infrastructure Sector or Key Asset/Resource [15]	PDD-63 (1998)	NSHS (2002)	NSPPCI (2003)	HSPD-7 (2003)	N.I.P.P. (2006)	N.I.P.P. (2009)	PPD-21 (2013) N.I.P.P. (2013)
DHS (Lead or Co-Lead)	N/A	5/14	9/18	10/18	10/17	11/18	10/16
	N/A	36%	50%	55%	59%	61%	63%

3.5. National Critical Functions:

The concept of the National Critical Functions (NCFs) recognizes that risk to infrastructure does not conform neatly to sector structures, and that systems and assets across multiple sectors are interdependent. In April 2019, CISA released a set of 55 NCFs, defined as the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

NCFs provide a functions-based approach to characterizing infrastructure risk—identifying the primary functions that infrastructure provides. These functions are delivered by systems and assets across multiple sectors. Vulnerabilities to critical infrastructure systems and assets can manifest in the loss or degradation of nationally critical functions, and the NCFs provide a framework for characterizing and responding to identified risks. As such, the NCFs provide a framework that encourages cross-sector coordination and a national lens through which to characterize infrastructure risk.

The NCFs are designed to serve as a cross-sector prioritization framework for infrastructure risk, establishing a mechanism for risk reduction coordination across all SRMAs. At the operational level, the NCFs will provide a framework and enhanced understanding of infrastructure for analysis and to help set priorities during incident management and response activities.

CISA has committed to engaging with critical infrastructure partners and other stakeholders to periodically review and, as necessary, update the existing set of 55 NCFs. Understanding how infrastructure relates to critical functions will improve the ability to identify infrastructure assets and systems that are most critical to the Nation’s day-to-day functioning. The NCF approach recognizes:

- Critical infrastructure risk is increasingly cross-sector in nature, and a siloed approach, particularly around cybersecurity, is no longer sufficient to manage risk.
- Understanding of risk must evolve from a static asset or organization view to include a more nuanced and holistic approach that also focuses on functions and services.
- Understanding and mitigating national-level risks requires more purposeful data collection and analysis methods.

- The need to broaden the stakeholder community involved in critical infrastructure risk management by better engaging groups not traditionally considered part of the infrastructure community.

Since their inception, NCFs have been leveraged for cybersecurity and critical infrastructure risk management doctrine. Specifically, NCFs are featured in the 2019 National Cyber Strategy, the 2020 DHS Cybersecurity Strategy, and the National Strategy to Secure 5G. Similarly, the Executive Order on Coordinating National Resilience to Electromagnetic Pulses leverages the definition of NCFs to call on the critical infrastructure community to better understand the effects of electromagnetic pulses) through assessment and prioritization of NCFs.

In day to day usage, CISA is working to ensure that the NCFs illuminate how infrastructure systems deliver products and services, assist in identifying and clarifying shared or consolidated risks, and prioritizing which systems and assets should be priority focus areas for risk reduction efforts.

3.5.1. Coordinating the NCF Framework

CISA, in coordination with SRMAs, will lead efforts to apply the NCF framework through the partnership structure detailed in the National Plan.

Ongoing efforts to define, understand, analyze, and prioritize risks to NCFs will be done in an iterative manner with sector partners, who will support validation of findings. This work will be governed by an appreciation of the various levels of information that may be available for each NCF; the number of sectors that may compose each NCF community of interest; the need to maintain proper protection of sensitive information; and continuing development and maturation of processes, tools, and reporting practices that will support a risk management framework focused on NCFs.

Prioritization and implementation of collective risk management activities focused on mitigating high-priority risks affecting NCFs will be undertaken collaboratively with relevant stakeholders; consistent with the nature of the risk and with relevant authorities and legal requirements; and where appropriate balanced with existing sector, jurisdictional, or organizational-level risk management activities.

CISA will coordinate with SRMAs and NCF communities of interest as they are established to identify appropriate performance indicators for functions and to evaluate the effectiveness of risk-management responses.[17]

3.6. Critical Infrastructure Environment

[17] U.S. Department of Homeland Security, Cybersecurity and Critical Infrastructure Security Agency, "National Critical Functions", June 20th, 2021. https://www.cisa.gov/national-critical-functions

The Homeland Security Act, as amended and codified in 6 U.S.C. §652, requires DHS to produce a comprehensive national plan to secure the Nation's critical infrastructure and key resources. As highlighted by the *National Security Strategy of the United States of America*, potential adversaries are developing advanced weapons and capabilities that could threaten U.S. critical infrastructure. Adversaries may also strategically target attacks to exploit interdependencies between infrastructure sectors and magnify cascading failures between them, posing incident response challenges above and beyond those created by earthquakes or other catastrophic natural hazards. The National Plan developed pursuant to 6 U.S.C. § 652(e)(1)(E) must address these challenges through a renewed and updated approach to ensuring that, through national and international partnerships, government and industry can coordinate to ensure the security and resilience of the Nation's critical infrastructure.

Securing infrastructure is not a purely public or private effort. Government and industry entities each own and operate portions of the critical infrastructure domain. Likewise, the information necessary to understand threats and vulnerabilities to infrastructure is distributed, and the risks associated with damaged infrastructure affect national security, economic security, and public health and safety. For these reasons, the National Plan must rely on an effective partnership model necessary for managing the shared complexity of infrastructure risk. This partnership model must leverage the appropriate legal authorities, policy tools, strategic collaboration mechanisms, and operational coordination mechanisms to facilitate the collective efforts of public and private sector entities across sectors and jurisdictions, including federal, state, and local levels.

The National Plan was last updated in 2013 when PPD-21 directed key improvements related to the risk management framework for security and resilience, methods to be used to prioritize critical infrastructure, protocols to be used to synchronize communication and actions among federal partners; and processes to be used to measure the Nation's ability to manage and reduce risks to critical infrastructure. The 2013 version has served as the National Plan for securing the Nation's infrastructure for the last eight years. Numerous changes in the policy and operating environments for critical infrastructure, as well as a complex and rapidly changing risk environment have created a demand for an updated national plan.

Since the National Plan was last published in 2013, the number and nature of threats and hazards the United States faces has grown more complex. As a nation, we are responding to increasingly sophisticated and frequent manmade threats and attacks from nation-states, cyber criminals, domestic violent extremists, terrorists, and opportunists. Natural hazards caused by severe weather and influenced by climate change are an increasing threat. Incidents such as the COVID-19 pandemic highlight our reliance not only on physical assets and systems, but on the essential workers that operate those systems. Many of these threats are occurring at the same time, adding to the complexity needed in response. Critical infrastructure vulnerabilities are also increasing in number and intricacy due to factors such as complexity in interconnected systems, new

technologies, and changing workforce demographics. As a result, consequences are on a growth trend. In an attempt to keep pace with this risk environment, the policy environment is rapidly changing, and requires agility and cooperation within and between jurisdictions to ensure responsible practice within the operating environment. Cross-cutting opportunities and challenges abound requiring strength and agility in collaborative partnerships and advanced planning needed to address the concerns of today and tomorrow.

Critical infrastructure sectors and individual organizations frequently have well-established risk management approaches. Risks that impact multiple sectors or organizations, however, remain a significant risk management challenge because there is frequently a gap in the collective ability to understand them and the governance mechanisms to implement and monitor joint risk management activities. These kinds of risks call for solutions beyond the capabilities of a single entity and require collaboration structures reflecting the shared responsibilities across sectors and communities. Collaboration, communication, and coordination can support joint and unified analysis and risk management approaches across sectors, jurisdictions, and even national borders.

3.6.1. Policy Environment

Security and resilience issues related to the Nation's infrastructure are influenced by the policy and regulatory environment. Engineering, performance, and design standards; voluntary security standards; federal, state, and local requirements; industry standards; market demands; economic conditions; international norms; and federal policy all shape the way that infrastructure owners, operators, and stakeholders make decisions and tradeoffs about how to secure infrastructure against risks. The policy environment since 2013 has shifted, as accidents, attacks, and disasters have each revealed increasingly important local, national, and international relationships between policy and practice.

Congress and several administrations have taken sustained action to enhance the security and resilience of infrastructure, including the enactment of laws, determination of policies, and establishment of federal agencies and programs dedicated specifically for the mission. The expanding scale of public risks revealed in chemical and nuclear safety failures—including the Bhopal and Chernobyl disasters in the 1980s—clearly illustrated the profound costs and shared risks of infrastructure failures. Efforts in the United States accelerated and expanded in the 1990s in parallel with a sequence of events and trends that included the collapse of the Soviet Union and associated fear of "loose nukes" that could target American cities, a series of major terrorism attacks against infrastructure, two catastrophic hurricanes, and the expansion of the Internet and associated concerns about cyberattacks on infrastructure. Previous concerns were later validated and exacerbated by the September 11th terrorist attack, the rise and diffusion of international terrorist groups and those inspired by them, a series of hurricanes and natural disasters with unprecedented impacts, increasingly frequent mass shootings and domestic terrorism, and other significant events.

National security policy discourse and decisions during the 1990s began to emphasize the need for better infrastructure protection and domestic preparedness. Reforms and continuous lessons learned since the September 11th attacks continued that trajectory. Significant laws and policies established in the wake of events and in response to evolving risk form the foundations for the infrastructure mission today: Figure 1 highlights key, but not exhaustive, policy developments in infrastructure security.

Figure 1: Summary of Critical Infrastructure Policy Between 1995 and 2018

- **Presidential Decision Directive 39, U.S. Policy on Counterterrorism (PDD-39)**, was issued two months following the Oklahoma City bombing, establishing formative, enduring policy emphasis on federal facility security, critical infrastructure protection, transportation security, explosives/weapons of mass destruction (WMD) security and incident response, national preparedness, and interagency coordination that remains highly relevant to the Infrastructure Security Division's (ISD) mission today (1995).
- **Executive Order 13010, Critical Infrastructure Protection**, was issued in 1996 following the Oklahoma City bombing and established the President's Commission on Critical Infrastructure Protection (PCCIP, or the Marsh Commission).
- **The Marsh Commission's Report of the President's Commission on Critical Infrastructure Protection** was issued in 1997 and specifically focused on threats to U.S. infrastructure and described them as falling into one of two categories—bombings/WMDs and cyberattacks.
- **Presidential Decision Directive 62, Combatting Terrorism (PDD-62), and Presidential Decision Directive 63, Critical Infrastructure Protection (PDD-63)**, were issued together in 1998 and continue to emphasize cybersecurity, infrastructure security, bombings/WMDs, and the value of public-private partnerships.
- **Executive Order 13231, Critical Infrastructure Protection in the Information Age**, was issued following the 9/11 attacks to ensure protection of information systems, including emergency communications, and the physical assets that support the systems, and established the President's Critical Infrastructure Protection Board and National Infrastructure Advisory Council.
- **Executive Order 13234, Presidential Task Force on Citizen Preparedness in the War on Terrorism**, was issued following the 9/11 attacks to identify, review, and recommend appropriate means by which the American public could prepare in their homes, neighborhoods, schools, places of worship, workplaces, and public places for the potential consequences of any possible terrorist attacks within the United States.
- **Homeland Security Act of 2002 (Public Law 107-296 as amended)**, created DHS and authorized and defined activities and programs that include, for example, critical infrastructure protection, national preparedness, information sharing, and public-private partnerships. The law requires CISA "To develop, in coordination with the Sector-Specific Agencies with available expertise, a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency communications systems, and the physical and technological assets that support those systems."
- **Homeland Security Presidential Directive 5, Management of Domestic Incidents (HSPD-5), Homeland Security Presidential Directive 7, Critical infrastructure Protection (HSPD-7), and Homeland Security Presidential Directive 8, National Preparedness (HSPD-8)** were issued in 2003 to establish national policies for national incident management, prioritization and protection of critical infrastructure, and the goals and processes for strengthening preparedness for major incidents. These HSPDs built upon guidance for incident management, infrastructure protection, and preparedness established in Presidential Policy Directives (PPD) -39, -62, and -63 and the Homeland Security Act. HSPD-8 was later replaced by Presidential Policy Directive 8 (PPD-8) in 2011; PPD-8 provided updated guidance and direction on achieving national preparedness and, in defining the components of national preparedness, referenced critical infrastructure preparedness as one component of the nation's overall security and resilience.
- **Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (PPD-21)**, was issued in 2013 to advance national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure—replacing HSPD-7 and defining critical infrastructure sectors, SSAs, and a national partnership structure.
- **Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure**, were issued in 2013 and 2017, respectively, to improve critical infrastructure cybersecurity, directing the Executive Branch to take a wide range of security and resilience steps focused on critical infrastructure.
- **Presidential Policy Directive 41, United States Cyber Incident Coordination (PPD-41)**, was issued in 2016 to set out an architecture governing the Federal Government's response to cyber incidents.

There have been many policy updates impacting the understanding and securing of the Nation's critical infrastructure. Although PPD-21, EO 13636: *Improving Critical Infrastructure Cybersecurity*, and PPD-8: *National Preparedness* are still in effect, the related policies and doctrines continue to evolve. For example, since the publication of the National Plan in 2013, the concept of Community Lifelines and NCFs have been developed as tools for understanding and managing homeland security emergencies and risk; Election Infrastructure was added as a subsector under Government Facilities; multiple Emergency Support Functions (ESFs) under the National Preparedness System have undergone revision or been added, including ESF #14: *Cross-Sector Business and Infrastructure*, to align and support cross-sector operations among infrastructure partners and stakeholders to stabilize community lifelines as well as any impacted NCFs; the Disaster Recovery Reform Act of 2018 emphasizes the Federal Emergency Management Agency's (FEMA) Threat and Hazard Identification and Risk Assessment (THIRA) approach for capabilities-based planning across the preparedness spectrum; and through the CISA Act of 2018, codifying responsibilities articulated in PPD-41: *United States Cyber Incident Coordination*, CISA became the federal lead for national cybersecurity asset response activities.

The National Plan and the National Response Framework both emphasize that SRMAs have incident management and national preparedness responsibilities, but historically, these roles and the alignment between the National Plan and the National Preparedness System have not been explicit. Additional work led by DHS to identify and implement improvements to the ESF structure would benefit the Nation's emergency response capabilities.

3.6.2. Operating Environment

The infrastructure operating environment is one increasingly defined by rapid technological shifts, dynamic competition, changing market conditions, and expanding security challenges. Lower barriers to entry for hostile actors, especially in the cyber domain and supply chain, have meant increased exposure to large scale risks, while emerging technologies and an unfolding global pandemic have shifted how infrastructure owners and operators conduct business and manage critical functions. The Nation's critical infrastructure has become much more complex, remains strongly interdependent; and continues to move from an operating environment characterized by discrete assets, systems, and networks to entwined functions and collaborative operations. Increasingly, the services and benefits provided by the different critical infrastructure sectors are affected by their own interdependencies and their complex supply chains, many of which are international. This increasingly complex environment requires effective collaboration mechanisms within and across sectors, as well as across jurisdictions and national borders, to increase the security and resilience of the Nation's critical infrastructure.

Nationally significant incidents have also driven closer operational coordination between the

critical infrastructure collaboration structures and the National Preparedness System. A main example is the establishment of ESF #14, which focuses on engaging private sector interests and infrastructure owners and operators—particularly those in sectors not currently aligned to other ESFs. The objective of ESF #14 is to support the coordination of multi-sector response operations between (or across) the government and private sector for natural or human-caused incidents that jeopardize national public health and safety, the economy, and national security (e.g., Tropical Storm Zeta, COVID-19 vaccine distribution).

Because of the dynamic nature of the operating environment, the ability to consistently partner to take advantage of unique skills and capabilities on both the public and the private sector remains the foundation for critical infrastructure security and resilience efforts. This collaboration must be facilitated by establishing the structures and processes necessary for government entities and industry to communicate freely without releasing proprietary information or providing unfair advantage.

4. FINDINGS

4.1. Overview

Evaluating the current framework for securing the Nation's critical infrastructure underscores aspects of the national effort that are essential to its success, and equally spotlights aspects that limit the success of the existing approach and are in need of refinement. Understanding both the policy history that underlies the current framework and the rationale behind it helps make sense of constraints and capabilities comprising the national effort.

Sectors continue to serve as a rational model for aligning federal security and resilience authorities, capabilities, and partnerships with industry to particular segments of the economy. However, the rapidly changing nature of infrastructure risk, technology, and economic activity have demonstrated that the bureaucratic and policy structures of risk governance (i.e., executive policy, sectors, and designated federal agencies responsible for them) adapt at a necessarily slower rate. Such shifts have further illustrated limitations and gaps in the tools and doctrine that guide and describe the federal role in critical infrastructure security, as well as created inefficiencies.

SRMAs (formerly SSAs) are a vital component of the national structure to manage risks to critical infrastructure, both in steady state and in response to a crisis. However, the capacity for the national approach through a National Coordinator and SRMAs to jointly identify, prioritize and realize concrete reductions in risk, and to carry out the responsibilities previously defined in policy and now codified in law, is inherently limited. These limitations include:

- the lack of collective, centralized resources and authorities to collect information rapidly, efficiently, and effectively in steady state and emergent situations;
- the difficulty in surveying the sector(s) to collect metrics and evaluate progress in reducing/mitigating risks to critical infrastructure planning and risk reduction activities with industry; and
- a national planning approach that has established priorities through sector specific plans, but has de-emphasized measurable federal implementation actions, including assessments, analysis, and risk reduction actions.

This section outlines key issues and findings regarding the current national approach.

4.2. Key Issues and Findings

4.2.1. National Governance and Interagency Coordination

The earliest comprehensive federal infrastructure security policy identified a federal approach that relied on a National Coordinator, sector liaison agencies, and special function agencies. While bold Federal Government changes and significant investments are needed to defend the vital functions of critical infrastructure that underpin the American way of life, this organizing approach remains

sound. Organizing the federal approach to infrastructure security into sectors relies on inherent authorities, expertise, and capabilities within federal departments and agencies designated as SRMAs, and provides a coherent scheme for private-sector partners to engage with government, share information, coordinate, and jointly work to reduce the risks to the Nation's infrastructure.

A key part of national governance and interagency coordination to protect the Nation's critical infrastructure is harnessing the capabilities of the U.S. Intelligence Community (IC). Such capabilities are indispensable to assessing foreign threats to critical infrastructure, developing warnings and alerts, and supporting assessment of vulnerabilities and development of resilience and response options. CISA and the SRMAs should work closely with DHS's Office of Intelligence and Analysis, the Office of the Director of National Intelligence, the Federal Bureau of Investigation, and the other elements of the IC to improve on existing methods and relationships; and to further inform the development and dissemination of intelligence-informed alerts and guidance to the owners and operators of critical infrastructure.

A partnership-based approach remains the most effective model for securing the Nation's critical infrastructure. However, those efforts must be augmented by regulatory authorities, standards-setting bodies, and a united federal approach to utilizing contracts for service providers, manufacturers, and others doing business with the government to adopt and maintain preparedness, security and resilience, information sharing and other requirements. While the ownership and operation of critical infrastructure are distributed across public and private sectors, the risk of losing national critical functions that infrastructure provides is shared by the entire Nation.

Wholesale changes to the sector structure and alignment to SRMAs have typically occurred through updated federal policy (e.g., PDD-63, HSPD-7, PPD-21). However, additional sectors and subsectors have also been added or removed outside of updates to Executive Branch policy. Since the creation of DHS, changes to the sector structure have largely assigned new sectors to DHS as the SRMA.[18] At present, DHS is the SRMA for 10 (Sole SRMA for eight, co-SRMA for two) out of the 16 current sectors. For example, in 2017 the Secretary of DHS established Election Infrastructure as a critical infrastructure subsector within the Government Facilities Sector.[19]

PPD-21 offers a general mechanism for modifications to the sector structure and designated SRMAs, providing that "The Secretary of Homeland Security shall periodically evaluate the need for and approve changes to critical infrastructure sectors and shall consult with the Assistant to the President for Homeland Security and Counterterrorism before changing a critical infrastructure

---

[18] See Table 5 above.

[19] Department of Homeland Security, "Statement by Secretary Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

sector or a designated SSA for that sector."[20] However, the rationale and approach for application of this process has varied, including modifications of the sector structure due to emerging risks, changing economic conditions, and shifts in technology. Amendments to the Homeland Security Act pursuant to the FY2021 NDAA include more formalization of this process as part of regular—and now required—updates to the National Plan. However, there remains a significant gap in formal process, procedure, criteria, and cycle for managing the designation of sectors and SRMAs.

Applying consistent criteria to how sectors and SRMAs are identified and designated will ensure that the national critical infrastructure framework relies on all the necessary capabilities and authorities across federal departments and agencies and does not overly rely on a single department's or agency's authority for managing sector engagement.

The comprehensive National Plan required pursuant to 6 U.S.C. §652 (e)(1)(E) has provided a vital framework for national coordination but must be updated in order to fulfill the intent of the changed authorities and policy surrounding SRMAs. The Homeland Security Act 6 U.S.C. §652(c)(4) requires the CISA Director to coordinate a national effort to ensure the security and resilience of the Nation's infrastructure, consistent with a comprehensive national plan also required in 6 U.S.C. §652. The law requires CISA to develop this plan "in coordination with the Sector Risk Management Agencies" [6 U.S.C. § 652 (e)(1)(E)]. Since the publication of the 2013 National Plan, significant changes in policy, the risk environment, and implementation have occurred. CISA and the Cross-Sector Council began a national effort in 2020 to update the plan, reemphasizing statutory and policy tools and definitive actions needed to coordinate a national infrastructure security and resilience strategy, and produced a draft in concert with all 16 current sectors, public, and private sector partners.

Yet there are still unresolved policy and process challenges. The definition of "Sector" is not codified in law or formalized in federal policy. This has created a challenge in clarifying and building criteria for clarifying and rationalizing the sector structure. The existing operating definition of "Sector," "[a] logical collection of assets, systems, or networks that provide a common function to the economy, government, or society," derives from the National Plan.

Similarly, there is no agreed upon definition of "subsector." CISA created the Infrastructure Data Taxonomy (IDT) to serve as a nomenclature that can be used by the infrastructure protection community and industry partners to categorize infrastructure assets and establish a common language for all to utilize. IDT establishes a detailed and structured terminology that facilitates data discovery, management, and enables data sharing among mission partners and systems. However, taxonomy assignments are based on the DHS Infrastructure Taxonomy V.4, issued in June 2011, and do not reflect changes to the taxonomy outlined in PPD-21, issued in February

[20] Presidential Policy Directive -- Critical Infrastructure Security and Resilience | whitehouse.gov (archives.gov)

2013, nor do they reflect subsequent changes to the Homeland Security Act.

As of April 2021, CISA is initiating an update of the IDT to ensure it reflects the current realities of the critical infrastructure space. The taxonomy will be updated in an iterative process, with continuous engagement of stakeholders across the infrastructure protection community.

The approach for designating or establishing subsectors within sectors is tailored to the specific needs and discretion of each sector, and varies widely between sectors, as do the corresponding functions and coordination mechanisms (e.g., Sector Coordinating Councils [SCCs], Government Coordinating Councils [GCCs], Information Sharing and Analysis Centers [ISACs]). Some sectors convene coordination mechanisms for subsectors, with others convening similar working groups or coordination efforts, but using different terminology.

In order to improve the ability of the sectors to manage risk nationally. 6 U.S.C. §652a now provides a standard approach by which the Secretary of DHS, in consultation with the Director and the heads of SRMAs, periodically reviews and makes recommendations to the President for modifying the sector structure. This includes revisions to the list of sectors and subsectors, and the designation of any Federal department or agency designated as the SRMA. There is an opportunity to clarify how the Secretary will coordinate this process with SRMAs, and formalize criteria and procedures for formalizing changes to the sector structure, and the National Infrastructure Protection Plan.

> **Finding 1.** CISA can improve national governance by maturing its role as the National Coordinator of activities to secure and protect against critical infrastructure risks under 6 U.S.C. § 652(c)(4) and clarifying the processes to modify sector and SRMA designations and assess sector maturity and remain nimble and adaptable to changing risks.

4.2.2. National Critical Infrastructure Sector Partnership Framework

National security risks associated with critical infrastructure do not necessarily conform to sector structures. For this reason, the national critical infrastructure sector partnership framework requires an approach to risk that encourages analysis and risk management activity that spans sectors and recognizes that risks originating in one sector can affect another and vice versa. The NCF approach is a response to this requirement.

Risks change faster than sector structures. The rate of change for national security risks, economic shifts, and technological advancements outpaces the adaptability of bureaucratic structures—including modifying the number and composition of the sector structure or the alignment of sectors to SRMAs.

In parallel to the periodic refining of the sector structure, policy has also called for an equally robust effort to enhance infrastructure prioritization schemas, resulting in a variety of different lists

of critical assets. Individual SRMAs are best situated to understand and characterize the scope of their sector, and the composition of specific systems and assets. Understanding the critical infrastructure that provides nationally critical functions is crucial to prioritizing and identifying vulnerabilities to that infrastructure. These efforts to identify the most critical assets, systems, and functions continue to complement the sector structure with current efforts focused on defining and identifying systemically important critical infrastructure for prioritized risk management focus.

Prioritizing specific infrastructure assets, systems, or functions occurs within and across the various sectors regardless of sector composition, resulting in a class of infrastructure with special status as a result of their importance to the overall functionality of infrastructure. The Homeland Security Act requires CISA to maintain a national asset database of critical infrastructure, along with prioritized lists of critical infrastructures. Likewise, the Homeland Security Act requires SRMAs to provide CISA with critical infrastructure information as part of the coordinated national effort to secure the Nation's infrastructure.

DHS, in coordination with relevant SRMAs, annually identifies and maintains a list of critical infrastructure entities that meet the criteria specified in EO 13636, Improving Critical Infrastructure Cybersecurity, Section 9(a) (“Section 9 entities”) utilizing a risk-based approach. Section 9 entities are defined as "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security.” Similarly, as directed by President Trump in EO 13800, DHS identified authorities and capabilities, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, and the heads of appropriate SRMAs, that the Federal Government could employ to support the cybersecurity efforts of Section 9 entities.

The Homeland Security Act now requires regular updates to the comprehensive National Plan for securing the Nation’s infrastructure and an assessment of the current sector structure at least every five years. Federal agencies will need to balance the need for adapting to shifts in risk, economy, and technology, with the requirement to authoritatively manage those changes.

The current 16-sector structure and associated SRMA designations have proven effective in promoting collaboration and fostering coordination between government and industry; however, modifications are needed to better reflect changes in national security risk, shift in global economic activity, and technological advancements. It is important to consider that, compared to other nations, the number of critical infrastructure sectors identified by the United States is well above the average number, as shown by an international survey conducted in 2018 by the Organization for Economic Cooperation and Development. Although the sector structure must be granular to accurately reflect the critical infrastructure landscape, an unnecessarily large number of sectors could potentially lead to fragmentation of efforts and lost opportunities for efficiencies.

The Homeland Security Act as amended now requires regular assessment and updates to the sector

structure and SRMA designations as needed. A periodic evaluation to confirm or modify the SRMA-sector alignment 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. Ideally, this evaluation should be conducted for all sectors (and subsectors). However, given the complexity of such an analysis, this report recommends a sequential approach to execute this evaluation. Conducting an evaluation through a phased approach will also allow validation and refinement of the corresponding methodology before potentially extending the evaluation of other sectors. This report recommends three groups of sectors (described in Section 5.2 below) and SRMAs for assessment based on statutory and policy authority. Each of these considerations warrants further assessment and analysis.

Other important aspects related to the sector structure are associated with the scope of the sector itself. In some cases, the name of the sector may not accurately capture the landscape (as in the case of the **Government Facilities Sector**, whose name is not fully accurate as the sector covers a broader range of critical functions than facilities). In other cases, multiple sectors offer a fragmented or partial view of a larger scope associated with common functions and therefore it may be advantageous to consider merging or consolidating those sectors (as in the case of the **Emergency Services Sector**, which contains services largely provided or overseen by government entities).

Finally, there is a need to incorporate more agile mechanisms to foster operation coordination and risk management collaboration across sector structures. For example, data management is currently a significant gap in the current critical infrastructure framework. The Homeland Security Act requires SRMAs to provide the director of CISA with critical infrastructure information. Likewise, the Secretary of DHS has specific responsibilities for maintaining a National Asset Database, and prioritized lists of critical infrastructures. Underpinning these and other requirements for infrastructure security is the need for a comprehensive infrastructure data management approach—including modernizing the existing IDT and standardizing the kinds of data that SRMAs provide, along with offering clear tools and processes for transmitting that data. Similarly, construction and infrastructure development support activities are currently not covered by the critical infrastructure framework. It is important to increase the flexibility of the existing collaboration framework to account for the need to work with those segments that are critical infrastructure supporting elements (or enablers) that are not necessarily aligned to any specific sector.

> **Finding 2.** The Federal Government can improve coordination and implementation of the national effort to secure the Nation's infrastructure.

4.2.3. SRMA Function

The roles and responsibilities of SRMAs, previously identified in federal policy, are now codified in law. PPD-21, and its predecessors HSPD-7 and PDD-63 have each noted the importance of special function agencies—federal agencies with roles and responsibilities essential the national effort and complimentary of SRMA roles and responsibilities. Although PPD-21 and, more recently, the FY2021 NDAA, have provided general guidance to SRMAs as to the primary components of their mission, significant differences in statutory authorities and among the critical infrastructure sectors have yielded varied approaches to the implementation of this mission. SRMAs would benefit from a greater degree of foundational consistency in how to execute the corresponding roles and responsibilities and how to coordinate to both avoid duplication of effort and ensure due consideration of interdependencies. To maximize the benefits of a fully coordinated approach, the roles and responsibilities of other PPD-21 agencies not currently designated as SRMAs should also be clarified.

Ensuring that SRMAs can meet these responsibilities requires a unified effort to clarify operational relationships, procedures, and MOUs for delivering SRMA responsibilities. For example, the law requires SRMAs to provide the Director of CISA with critical infrastructure information (as defined in 42 U.S.C. § 5195c) but leaves to federal agencies the responsibility for clarifying and organizing the kinds of information shared, and the processes for acting on that information. Similarly, SRMAs have codified emergency preparedness and incident response roles and responsibilities, but the doctrine and practice linking PPD-21 to PPD-8 and the National Preparedness System are still under development. SRMAs produce various products and services, with some choosing to engage heavily on emerging topics such as essential workers and others electing to prioritize other work.

Some SRMAs are also coordinators or primary/lead agencies for Emergency and Recovery Support Functions within the National Preparedness Framework, and the roles and responsibilities are not well distinguished between the sector and the ESF domains. The recently established ESF #14 supports the coordination of cross-sector operations, including stabilization of key supply chains and community lifelines, among infrastructure owners and operators, businesses, and their government partners. ESF #14 is complementary to the SRMAs and other ESFs and is a mechanism for entities that are not aligned to an ESF or have other means of coordination. While those aligned with specific ESFs typically use them as their primary interface, participating in ESF #14 allows for cross-sector collaboration and problem-solving during complex emergencies. ESF #14 serves as the primary interface for unaligned sectors and supports coordination among all sectors. SRMAs that also have responsibilities as lead, coordinating, or supporting federal agencies for ESFs within the National Preparedness System and associated Federal Interagency Operational Plan for Response require clearer delineation of SRMA specific responsibilities for incident management and preparedness during steady state and crisis.

More broadly, the roles and responsibilities associated with the execution of the SRMA function

have varied over time and between SRMAs. Given the interdependent nature of our critical infrastructure, it is imperative that SRMAs work together through the National Plan, and the CISA Director's role as National Coordinator. Establishing doctrine and plans subordinate to the National Plan will enhance the ability of SRMAs to efficiently execute their responsibilities, and strengthen the effort described in the National Plan. This is particularly important in cases where SRMAs must coordinate on infrastructure that spans or supports multiple functions across infrastructure sectors—including industrial control technologies, operating technologies, etc. Presently, more than one federal agency shares SRMA functions within some sectors, serving as "co-SRMAs" for their respective sectors. PPD-21 and the Homeland Security Act do not describe this shared responsibility approach, and further doctrinal delineation of these responsibilities will help clarify the role of individual SRMAs.

SRMAs require greater consistency in the identification of risk to their sector, collaboration of interagency and dependency risk, and subject-matter expertise to evaluate, analyze and address the risk. Consistency in data collection, taxonomy, and risk methodology across sectors will allow for a national approach that can characterize infrastructure risk, identify trends and risks that span multiple sectors, and create a standard approach to understanding risk within individual sectors. There are opportunities to improve the alignment of federal programs to identify and prioritize critical infrastructure, to comprehensively assess its vulnerabilities, and develop analysis and proposed risk countermeasures through the SRMAs in a manner that appropriately relies upon centralized services provided by CISA wherever possible to minimize duplication of effort and promote cross-sector visibility. Likewise, there is an opportunity to harmonize and incorporate regulatory functions that relate specifically to each sector and SRMA into the risk approaches outlined in the National Plan. Pursuant to section 7(d) of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), the Secretary of Homeland Security, in coordination with the Secretary of Commerce (through the director of the National Institute of Standards and Technology) and other agencies, as appropriate, are also required to develop and issue cybersecurity performance goals for critical infrastructure to further a common understanding of the baseline security practices that critical infrastructure owners and operators should follow to protect national and economic security, as well as public health and safety.[21]

The Federal Government lacks an understanding of the full resources allocated to homeland security, as some agency programs may not be classified as homeland security in the budget process but may nonetheless support the agency's security mission. In addition, the Federal Government has not established baseline resource requirements or requirements analysis tools to

[21] White House, *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*, July 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

support SRMAs ability to estimate the costs necessary to perform their functions. This lack of baseline responsibilities, capability and resource requirements creates challenges for SRMAs when they must create and justify budgetary requests to fulfill their statutory roles as SRMAs. SRMAs—jointly, through CISA as the National Coordinator and the Office of the National Cyber Director—

> **Finding 3.** SRMAs require greater consistency in resources and doctrine, which would reinforce SRMA operations, enable the development of clearer objectives and performance goals, and improve coordination with other key Federal agencies and partners.

should collectively engage the Office of Management and Budget (OMB) to identify the government's budgetary requirements for fulfilling SRMA roles and responsibilities.

4.2.4. Effectiveness of Collaboration Mechanisms

For some critical infrastructure sectors, achieving progress in security and resilience depends on voluntary partnerships between government and the private sector. While voluntary partnerships are fundamental to the national effort, they retain some inherent limitations to drive actionable and measurable risk management efforts; these could be mitigated through additional approaches specifically targeting systemically important critical infrastructure and those who provide goods and services (such as information and communication technology, and operational technology enablers) to the Federal Government and critical infrastructure owners and operators. Current sector-based coordination structures are typically based on self-nomination or interest to participate from individual entities and not necessarily on specific functional roles or risk management responsibilities. This approach, while useful in creating robust partnerships, may lead to challenges in establishing collaboration structures that are fully equipped to execute and implement risk management activities that can measurably influence the national risk picture.

Similarly, while the current National Plan acknowledges that there are regulatory authorities and other tools inherent to the critical infrastructure security and resilience mission, the plan does not fully describe the way that regulatory and other tools interact with the voluntary partnership model to drive cohesive progress toward national goals. Voluntary coordination between the public and private sector is a core element of the national approach to critical infrastructure security. However, there are inherent limitations to purely voluntary approaches—a reality that is reflected in design and construction codes and standards as well as in regulatory authorities.

Many of the tools that SRMAs use to manage partnerships with the public and private sectors are designed to promote voluntary coordination and information sharing. This is because legitimate disincentives (e.g., reputational or regulatory disincentives, proprietary information risks) exist for partners to share critical infrastructure information with the Federal Government. The protections offered by the CIPAC framework as well as the legal protections and information handling

requirements associated with PCII, are designed to reduce these disincentives and encourage information sharing and joint action.

However, the Homeland Security Act, PPD-21, and the National Plan all recognize that regulatory authority and capability are central reasons that a federal agency would be designated as an SRMA within a given sector. Likewise, SRMAs and DHS have responsibilities to identify appropriate countermeasures to infrastructure threats and vulnerabilities.

The National Plan references mandatory security and resilience requirements, including performance and design codes and standards and regulatory authorities in the state, local and federal spheres. However, the National Plan does not fully describe how mandatory and voluntary approaches work together to ensure national infrastructure security. For the Federal Government to bring to bear the full scope of its authorities and resources, there is an opportunity to harmonize and incorporate regulatory functions, standard setting bodies, and other strategic methods that relate specifically to each sector and SRMA into the risk approaches outlined in the National Plan. Likewise, state, local, and independent entities also have authorities and resources that, for some sectors, can be more fully integrated into the public-private partnership efforts led by SRMAs through their role as chair of the corresponding GCC.

Sector-specific activity is the shared product of public- and private-sector efforts and coordination mechanisms. The variability in the success of achieving meaningful security goals in each sector is likely a function of the variable statutory and regulatory requirements applicable to each sector, though in some instances the ability to partner with private sector stakeholders may contribute to this success. While SRMAs have established methods and a baseline for the maturity of the partnership, no agreed approach exists for assessing sector effectiveness or SRMA capability and performance, and there is no uniform methodology to assess the effectiveness of the individual partnerships or the value the partnerships are providing to sector stakeholders.

> **Finding 4.** Voluntary coordination and partnerships are vital for information sharing and collaboration. However, a coordinated national effort to secure the nation's infrastructure can do more to directly inform, encourage, and coordinate cross-sector risk reduction actions.

4.2.5. Information Flow and Coordination

CISA and SRMAs share vulnerability, incident-specific, and other risk data. The National Plan serves as a strategic framework for this effort, but does not direct a unified infrastructure prioritization, assessment, analysis, and data sharing process to establish a comprehensive federal infrastructure security approach. SRMAs conduct intelligence and information sharing within and outside their sectors (including with private sector and SLTT entities) according to agency

authorities and sector-specific vehicles and mechanisms, but sector-specific approaches are not fully integrated to a national approach to unify the way that threat and vulnerability intelligence (classified, unclassified, and traffic light protocol sensitive) information is shared with industry partners across all sectors. In addition to sharing threat information, the Federal Government must provide concrete countermeasures that would enable sector partners to mitigate risk, and, moreover, provide a description of the countermeasures that is comprehensible to these partners. CISA must mature efforts to serve as a "hub" for cross-sector information sharing and analysis to minimize sectoral stovepipes and rapidly identify emerging risks across sectors that require exigent mitigation.

In spite of robust information-sharing efforts linking the established sector-specific and cross-sector structures, it is necessary to develop and implement approaches that reach beyond the membership of current councils, including regional stakeholders as well as entities that are not directly affiliated with any specific sector but are strategically important for steady-state or incident-related information sharing.

While CISA has initiated and established the NCFs as the national model for prioritizing and addressing infrastructure risk, the NCFs are not yet a shared national model across all SRMAs for prioritizing risk management activities and driving information sharing activities. The SRMAs require a standing vehicle to advocate for the types of intelligence and intelligence sharing processes that they would find most helpful to inform their work, including the facilitation of the identification of intelligence needs and priorities of critical infrastructure owners and operators across all sectors.

Efforts such as the framework developed by the FSLC Working Group on Federal Roles and Responsibilities for Critical Infrastructure Cybersecurity at the request of the National Security Council Cyber Policy Coordination Committee have been helpful in improving federal agency coordination with SRMAs, but similar efforts need to be examined across other threats and hazards and integrated into the National Plan. For some sectors, there is a need for establishing and carrying out programs that assist critical infrastructure owners and operators to increase coordination, assess sector-specific risk, perform impact analysis, provide information sharing and guidance on mitigation of threats, vulnerabilities, and risks. Information sharing efforts must be bi-directional and continuously assessed to ensure the information shared is relevant and supports decision making.

Finding 5. There is a need for stronger risk assessment, vulnerability analysis, information sharing, coordination mechanisms, and actionable countermeasures to manage cross-sector risks and incidents.

5. RECOMMENDATIONS

5.1. Recommendations regarding National Governance and Interagency Coordination

Finding 1. CISA can improve national governance by maturing its role as the National Coordinator of activities to secure and protect against critical infrastructure risks under 6 U.S.C. § 652(c)(4) and clarifying the processes to modify sector and SRMA designations and assess sector maturity and remain nimble and adaptable to changing risks in support of this role.

- CISA and the SRMAs, in collaboration with the Office of the National Cyber Director (ONCD), the National Security Council (NSC), should clarify federal roles and responsibilities for sector risk management and sector coordination, build processes to support its responsibilities as National Coordinator, and lead the implementation of the recommendations in this report, as appropriate.
    - This should include criteria and approaches—such as those presented in this report—for identifying and designating sectors and SRMAs.
    - This should include a review and recommendations to restructure the existing architecture of coordinating councils and its supporting governance framework to ensure effective and impactful collaboration between government and industry.
    - The effort should identify areas previously confined to policy that are now codified in law and adjust the scope of the policy appropriately.
- CISA and the SRMAs should leverage the Federal Senior Leadership Council (FSLC) to develop a process for modifying the sector structure and/or the corresponding SRMA designations.
    - The coordination process should account for the need to modify the sector structure outside the regularly scheduled review cycle.
- The FSLC should serve as an interagency consensus based decision-making body with oversight and governance responsibilities for the national effort.
    - The FSLC, whose membership should reflect all entities with federal equities in PPD-21 or its successor, including SRMAs and special function agencies, should serve as the primary interagency mechanism through which CISA should execute the assigned National Coordinator role.
- CISA should lead an FSLC Working Group to validate and implement the processes outlined in Appendices C and D of this report.
    - As such, modifications to the sector structure should consider the following factors, among others:

        - Evaluation of whether appropriate mechanisms for risk management coordination exist or can be established.
        - Consideration of functional risk to ensure that relevant risk drivers can be adequately addressed across the resulting critical infrastructure framework.
        - Evaluation of how effective the existing collaboration structures have been as well as an identification of opportunities for improvement.
    - The FSLC Working Group should also establish procedures for identifying, nominating, and ratifying changes to the sector structure and/or SRMA-sector alignment through updates to the National Plan.
- The FSLC should develop, and SRMAs should implement, a customizable methodology for each SRMA to assess the maturity and effectiveness of their sector-specific partnership structures.
    - The FSLC should conduct a sector-by-sector assessment of the effectiveness of the partnership structures, with a specific focus on private sector participation, and make recommendations for improvement.
    - The FSLC should develop and implement a standardized charter template for the GCCs and SCCs to ensure high-quality, consistent council performance.

  The results of such assessment should be included as part of the periodic update of the corresponding Sector Specific Plans.

5.2. Recommendations regarding the coordinated National Effort

Finding 2. The Federal Government can improve coordination and implementation of the national effort to secure the Nation's infrastructure by updating existing national and sector-specific plans, establishing risk management priorities for each sector, and providing guidance and resources to SRMAs to perform roles and responsibilities.

- CISA, in collaboration with ONCD, NSC, and the SRMAs, with input from other relevant departments and agencies, should update the National Plan, including clarifying the role of the NCF in establishing risk management priorities across sectors
    - The updated National Plan should emphasize the national partnership approach, the value of the CIPAC, PCII, and other tools designed to encourage information sharing, promote tools and capabilities for vulnerability disclosures, and describe a whole-of-government approach for securing critical infrastructure through partnership management; planning, analysis, and incident reporting; information sharing; capacity building; and incident response.
    - The updated National Plan should acknowledge that SRMAs often have authorities, responsibilities, and partnerships with SLTT and private industry that reflect the unique nature of their sector and extend beyond security and resilience issues. The SRMAs can play an important role in integrating response to the technical aspects of incidents with efforts to mitigate the systemic impacts resulting from those incidents. The updated plan should explicitly reference regulatory authority as criterion for SRMA designation given their existing authorities, responsibilities, and partnerships with private industry.
    - The updated National Plan should better acknowledge the federal and state departments and agencies that are not designated as SRMAs, but have unique responsibilities, functions, or expertise in a particular critical infrastructure sector.
        - For example, some sectors are regulated by federal or state regulatory agencies that are not the designated SRMA for the sector, but they possess unique insight into the functioning of the critical infrastructure they oversee and may bring key capabilities to the critical infrastructure partnership.
        - The updated National Plan should be consistent with the National Preparedness Goal to enable an integrated approach for building, sustaining, and evaluating core capabilities required to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.

    - The updated National Plan should reformulate and set joint and SRMA specific priorities and objectives within each planning cycle, with a view to aligning them with NCF dependency and sector boundaries suitable for ongoing assessment and capacity-building and for the auditing cycle established by the FY2021 NDAA.
- CISA, in collaboration with ONCD, NSC, and SRMAs, and with input from other relevant departments and agencies, should apply the framework outlined in this report to evaluate the scope of current critical infrastructure sectors to ensure they appropriately address systems, assets, National Critical Functions, and capabilities; evaluate potential modifications to SRMA designations; and evaluate the potential establishment of new sectors or subsectors.
    - This report recommends assessing the scope of the current sectors based on the criteria outlined in Appendix A. Additionally, taking into account the statutorily defined SRMA roles and responsibilities, and the corresponding requirement to align SRMA designations to authorities and capabilities of the department or agency in question, this report recommends for sectors to undergo an evaluation to confirm or modify the existing SRMA designation based on the criteria outlined in Appendices B, C, and D.
    - The evaluation of existing sector scope and SRMA alignment should occur in phases to ensure lessons learned from assessing one group can be incorporated in the subsequent one.
    - The effort should evaluate the establishment of the **Space Sector** as a critical infrastructure sector based on the criteria outlined in Appendix A. If the evaluation yields the need to establish a new sector, conduct the corresponding assessment to identify a department or agency as the potential SRMA based on the criteria outlined in Appendices B, C, and D.
    - The effort should evaluate the establishment of the **Bioeconomy Sector** as a critical infrastructure sector based on the criteria outlined in Appendix A. If the evaluation yields the need to establish a new sector, conduct the corresponding assessment to identify a department or agency as the potential SRMA based on the criteria outlined in Appendices B, C, and D.
- CISA should lead an effort through the FSLC to identify both cross-sector and individual sector risk management priorities.
    - The effort should address strategic collaboration through the established partnership structures as well as other more flexible multi-sector collaboration constructs focused on specific functional risks.
- CISA should lead an effort to expand and strengthen cross-sector coordination structures to address rapidly evolving or urgent risks.

- Cross-sector working groups can and should incorporate risks to the most critical assets, systems, and functions as identified through ongoing efforts to identify systemically important critical infrastructure, as appropriate.
- Working groups will be overseen by the corresponding SRMAs and CISA to avoid any duplication of efforts or conflicting outcomes resulting from these efforts.

5.3. Recommendations regarding the SRMA Function

> **Finding 3.** Guidance to inform the baseline of performance, resources, and doctrine required of SRMAs will help to reinforce SRMA operations, enable the development of clearer objectives and performance goals, and improve coordination of SRMAs with CISA and other key Federal agencies and partners.

- CISA should collaborate with SRMAs to improve processes and tools for carrying out their responsibilities in a manner that leverages subject matter expertise and unique understanding of their respective sector while also contributing to the cross-sector services provided centrally by CISA.
    - Through the FSLC, SRMAs and CISA should develop written doctrine and procedures documenting roles, responsibilities, and expectations associated with the execution of the SRMA function.
    - The FSLC should establish,coordinate, and review annual priorities, sector-specific goals supporting those priorities, and reporting requirements for CISA and SRMAs that consider the unique needs of each sector and capabilities of each SRMA.
- CISA should lead an effort through the FSLC to develop a baseline SRMA cost estimation approach to assist in budget formulation and to provide recommendations to the Office of Management and Budget (OMB) on the implementation of a consistent resource request process to support execution of SRMA responsibilities.
    - The tool, which should not represent a one-size-fits-all solution to the problem and should account for different maturity targets, should serve as a general baseline for resource estimation to be tailored by each SRMA in support of its roles and responsibilities.
- All SRMAs, coordinating through the FSLC, should update their sector-specific plans outlining specific authorities and capabilities, objectives, priorities, adding a five-year roadmap outlining key activities to be implemented in carrying out the responsibilities under 6 U.S.C. 665d.
- SRMAs require greater consistency in resources and doctrine that would enable the development of clearer objectives and performance metrics. Improved coordination between SRMAs and CISA, as well as other key agencies, presents an important opportunity to improve the federal government's role in protecting critical infrastructure.
- CISA should establish a National Coordinator assistance model to outline the provision of CISA resources to SRMAs for enhanced coordination and technical support for sector-level risk analysis.

5.4. Recommendations to Assess and Enhance the Effectiveness of Collaboration Mechanisms

> **Finding 4.** A coordinated national effort to secure the nation's infrastructure can do more to directly inform, encourage, and coordinate risk reduction actions.

- CISA, in coordination with the FSLC, should explore existing voluntary and regulatory mechanisms for risk reduction and then consider additional mechanisms that may be needed to incentivize and jointly develop and implement security and risk mitigation actions through the national partnership, incorporating and reflecting the risk reduction benefits of adherence to standards, best practices, and regulatory requirements.
- The updated National Plan should: 1) more fully address the integration and distinction of how regulatory authorities, standards setting bodies, contract requirements, and responsibilities impact the national effort to secure the Nation's infrastructure; and 2) inform SRMAs in their efforts to prioritize resources to manage risks.
    - CISA, in collaboration with ONCD, NSC, and SRMAs, and with input from other relevant departments and agencies, should conduct an interagency review of risk management mechanisms to incentivize implementation of security and risk mitigation actions.
        - This effort should include an evaluation of gaps and the potential need for new authorities (including analysis of current and/or new regulatory regimes)—consistent with the recommendations from the Cyberspace Solarium Commission—operationalizing the "systemically important critical infrastructure" concept and providing the Secretary in consultation with the heads of relevant SRMAs, where applicable, with the authority to designate high-priority infrastructure, target federal resources to designated infrastructure, and require certain actions from owners and operators of such.
        - Evaluation should include the critical protection, security, and resilience role played by owners of systems that process data (information technology [IT]) and those that run the vital machinery that ensures our safety (operational technology [OT]).
        - Evaluation should also include factors important to more secure, diverse, and resilient supply chains upon which critical infrastructure owners and operators rely.
        - Evaluation should carefully examine the proper jurisdictional scope of the authorities of the Federal Government and the associated impacts on state and local jurisdiction as appropriate by sector.

5.5. Recommendations to Enhance Information Flow and Coordination

> **Finding 5.** There is a need for stronger risk assessment, vulnerability analysis, information sharing, coordination mechanisms, and actionable countermeasures to manage cross-sector risks and incidents.

- The FSLC should address existing information sharing frameworks, interagency requirements and procedures for fulfilling statutory obligations to share information with relevant departments and agencies, information sharing cycles, and vulnerability and threat disclosure requirements.
- The FSLC should address multilateral infrastructure intelligence needs, key intelligence questions, Private Sector Clearance Program modernization, classified/unclassified/TLP tear line and information sharing procedures, and vulnerability and threat disclosure doctrine.
    - The effort should emphasize that information sharing efforts must be bi-directional and should be continuously assessed to ensure the information shared is relevant and actionable.
    - The effort should also address multilateral sharing of cybersecurity threat information from critical infrastructure owners and operators across sectors, including the development or clarification of standards and processes for sharing such information among owners and operators, the SRMAs, and CISA.
- The FSLC should evaluate Federal agency cyber incident response authorities, processes, roles and responsibilities, and cross-sector infrastructure roles and responsibilities.

Appendix A: DECISION-SUPPORT FRAMEWORK TO IDENTIFY CRITICAL INFRASTRUCTURE SECTORS

When evaluating the potential identification of a new critical infrastructure sector, CISA will coordinate with departments and agencies and ask and answer a series of questions to gauge the cohesion, importance, and capabilities of a prospective sector.

A critical infrastructure sector has two basic characteristics: it encompasses a collection of assets, systems, or networks and it provides common functions to the economy, government, or society.

However, the identification of a critical infrastructure sector requires a number of additional considerations beyond these two basic elements. One crucial aspect (which is tied to the homeland security perspective) is whether disruptions to the critical infrastructure sector under consideration or its associated functions lead to debilitating impacts on security, national economic security, national public health, or safety. Another key consideration is whether the spectrum of risks inherently associated with the potential sector are appropriately managed through existing frameworks (which may include multiple regulatory mechanisms, policies, or governance structures). Finally, and assuming there is an opportunity to enhance the overall risk management posture of the potential sector, it should be considered whether or not there is a need for (and a clear benefit that would result from) the type of collaboration mechanisms associated with critical infrastructure voluntary partnerships.

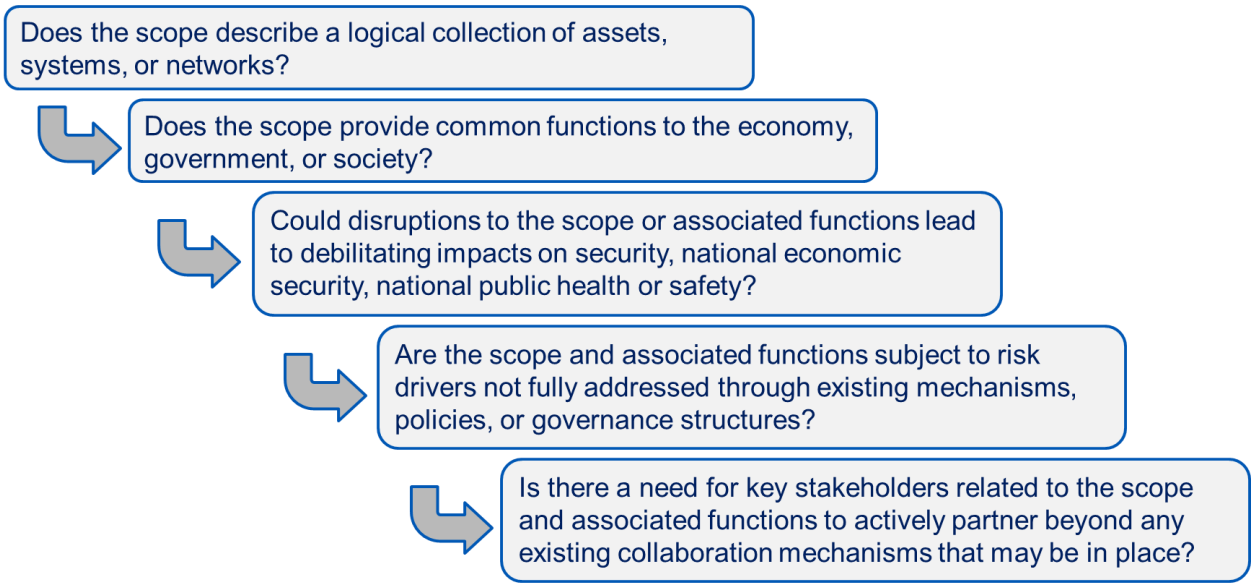
The critical infrastructure partnership structure is designed for coordinated national risk management, and reviews of the sector structure may be driven by exigent or emergent risks, changes in technology, or market forces. Because infrastructure sectors are a doctrinal, qualitative distinction, the decision to recommend changes to the sector structure is not purely quantitative but includes qualitative elements that address the best approach to incorporate new challenges into the partnership framework. Conducting a review of a potential sector must rest upon a careful deliberative approach that needs to include those stakeholders with relevant equities. This deliberation is therefore a process that may yield multiple alternatives, not a fixed algorithm leading to a binary answer (yes/no).

This type of evaluation should be conducted through a combination of CISA analytical work and consultation with key interagency and industry partners.

As described in the figure below, the process to drive potential changes to the sector structure should consider the following guiding questions:

1. Does the scope describe a logical collection of assets, systems, or networks?
2. Does the scope provide common function to the economy, government, or society?
3. Could disruptions to the critical infrastructure sector lead to debilitating impacts on security, national economic security, national public health, or safety?

4. Is the critical infrastructure sector subject to risk drivers not fully addressed through existing mechanisms, policies, or governance structures?
5. Do key stakeholders within the critical infrastructure sector need to actively maintain their partnership beyond any existing collaboration mechanisms that may be in place?



As previously mentioned, evaluating the need to make changes to the sector structure should rely on CISA analytical capabilities to consolidate relevant data and information associated with the guiding questions. This effort should also include a comprehensive stakeholder mapping to fully characterize the domain and extent of equities involved. This analytical work should then inform a deliberative phase with key stakeholders of the prospective sector. This deliberative process should yield a collective answer to each one of the guiding questions. If this process yields a positive answer to all of the guiding questions, then it should be recommended for the prospective sector to be officially designated as a critical infrastructure sector according to the appropriate designation procedure.

Appendix B: RESPONSIBILITIES OF SECTOR RISK MANAGEMENT AGENCIES

As amended by the *2021 National Defense Authorization Act*, Section 2201(5) of the *Homeland Security Act of 2002* defines an SRMA as "a Federal department or agency, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department."

Sec 2215(c) of the NDAA establishes that each SRMA shall utilize its specialized expertise to perform a number of responsibilities related to the designated critical infrastructure sector or subsector. These responsibilities include assessing sector risk, maintaining situational awareness, supporting sector risk management, executing sector coordination, conducting bi-directional information sharing regarding physical and cybersecurity threats, supporting incident management, and contributing to emergency preparedness efforts with industry and at the state, local, tribal, and territorial government levels. SRMAs will coordinate directly with state and local agencies relevant to their designated sector (e.g., public utility commissions).

The responsibilities assigned to SRMAs under the NDAA are aligned to those previously assigned SSAs under Presidential Policy Directive 21 (PPD-21). The responsibilities associated with providing sector-specific expertise, program support, and sector coordination are essentially the same as described in PPD-21. The most significant difference is that the NDAA makes explicit certain responsibilities that were largely implicit in PPD-21, such as the tasking for risk management and assessment, roles that were previously implicit under incident management and technical assistance and consultation. Under Sec 2215(c)(1) and (2), the NDAA explicitly tasks SRMAs with supporting sector risk management and assessing sector risk, duties which entail studying, assessing, and prioritizing risk; participating in national risk assessments led by DHS; and recommending security measures. Additionally, the FSLC, whose membership should reflect all entities with federal equities in PPD-21 or its successor, including SRMAs and special function agencies, should serve as the primary interagency mechanism through which CISA should execute the assigned National Coordinator role.

Relatedly, Sec 665d(c)(4) explicitly authorizes SRMAs to share threat and other critical infrastructure information (e.g., system architecture and design, vulnerabilities) of a physical and cyber nature, including identifying the intelligence needs of critical infrastructure owners and operators; exchanging relevant information within CISA and across the Federal Government; and promoting general awareness of threats within their respective sectors and other related sectors.

Sec 665d(c)(6) tasks SRMAs with supporting emergency preparedness efforts—a more proactive role than that previously assigned under the incident management tasking set out in PPD-21—by

coordinating across industry and government, participating in exercises, and contributing to planning documents (e.g., state energy security plans, mutual aid and assistance plans).

As described in law, the SRMAs are responsible to/for:

- Supporting sector risk management, in coordination with the [CISA] Director, including:
    - establishing and carrying out programs to assist critical infrastructure owners and operators within the designated sector or subsector of such sector in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets, or within a region, sector, or subsector of such sector; and
    - recommending security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets;
- Assessing sector risk, in coordination with the [CISA] Director, including:
    - identifying, assessing, and prioritizing risks within the designated sector or subsector of such sector, considering physical security and cybersecurity threats, vulnerabilities, and consequences; and
    - supporting national risk assessment efforts led by the Department;
- Sector coordination, including:
    - serving as a day-to-day Federal interface for the prioritization and coordination of sector-specific activities and responsibilities under this title;
    - serving as the Federal Government coordinating council chair for the designated sector or subsector of such sector;
    - participating in cross-sector coordinating councils, as appropriate;
- Facilitating, in coordination with the [CISA] Director, the sharing with the Department and other appropriate Federal department of information regarding physical security and cybersecurity threats within the designated sector or subsector of such sector, including:
    - facilitating, in coordination with the [CISA] Director, access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure, including through information sharing and analysis organizations and the national cybersecurity and communications integration center;
    - facilitating the identification of intelligence needs and priorities of critical infrastructure owners and operators in the designated sector or subsector of such sector, in coordination with the Director of National Intelligence and the heads of other Federal departments and agencies, as appropriate;
    - providing the [CISA] Director, and facilitating awareness within the designated sector or subsector of such sector, of ongoing, and where possible, real-time awareness of identified threats, vulnerabilities, mitigations, and other actions related to the security of such sector or subsector of such sector; and
    - supporting the reporting requirements of the Department under applicable law by providing, on an annual basis, sector-specific critical infrastructure information;

- Supporting incident management, including:
    - supporting, in coordination with the [CISA] Director, incident management and restoration, and recovery efforts during or following a security incident; and
    - supporting the [CISA] Director, upon request, in national cybersecurity asset response activities for critical infrastructure; and
- Contributing to emergency preparedness efforts, including:
    - coordinating with critical infrastructure owners and operators within the designated sector or subsector of such sector and the [CISA] Director in the development of planning documents for coordinated action in the event of a natural disaster, act of terrorism, or other man-made disaster or emergency;
    - participating in and, in coordination with the [CISA] Director, conducting or facilitating, exercises and simulations of potential natural disasters, acts of terrorism, or other man-made disasters or emergencies within the designated sector or subsector of such sector; and
    - supporting the Department and other Federal departments or agencies in developing planning documents or conducting exercises or simulations when relevant to the designated sector or subsector or such sector.

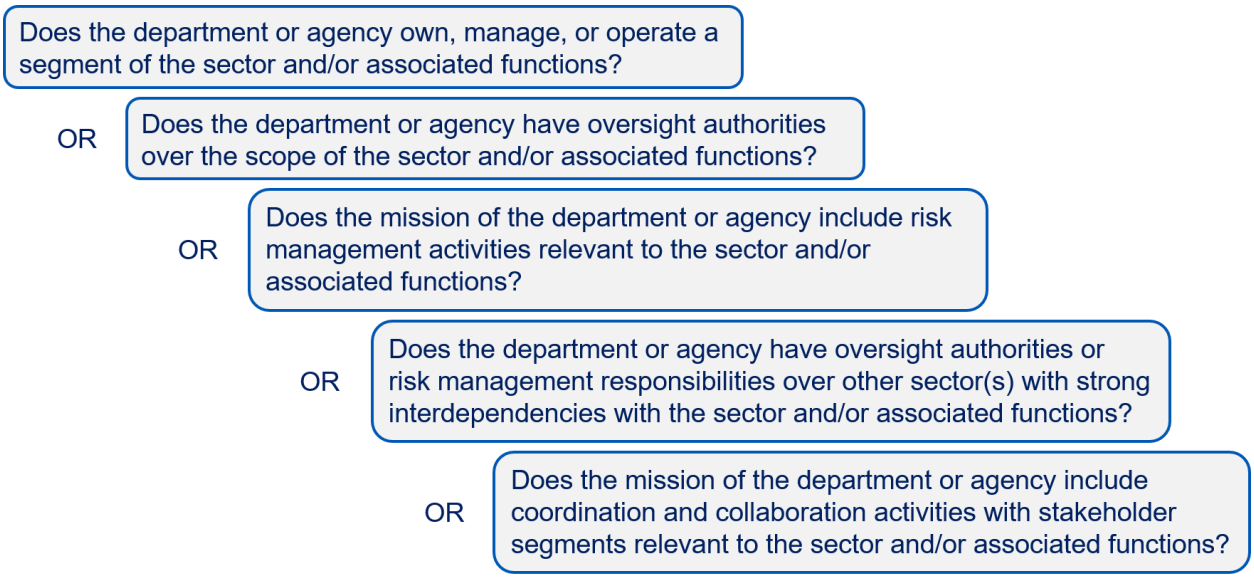
Appendix C: DECISION-SUPPORT FRAMEWORK TO IDENTIFY FEDERAL EQUITIES

Having the right organizations included in a public-private partnership is a key success factor. While SCCs are self-organized entities and are authorized to manage their own membership, GCC membership is under the purview of the National Plan Partnership Structure.

To identify if a department or agency should be member of a GCC, it is necessary to determine if the potential GCC meets federal equity criteria:

1. Does the department or agency own, manage, or operate a segment of the sector and/or associated functions?
2. Does the department or agency have oversight authorities over the scope of the sector and/or associated function?
3. Does the mission of the department or agency include risk management activities relevant to the sector and/or associated functions?
4. Does the department or agency have oversight authorities or risk management responsibilities over other sector(s) with strong interdependencies with the sector and/or associated functions?
5. Does the mission of the department or agency include coordination and collaboration activities with stakeholder segments relevant to the sector and/or associated functions?

The following figure summarizes the decision process that should guide this evaluation (Note: for certain federal entities, such as the Department of State, coordination equities exist for virtually all sectors):

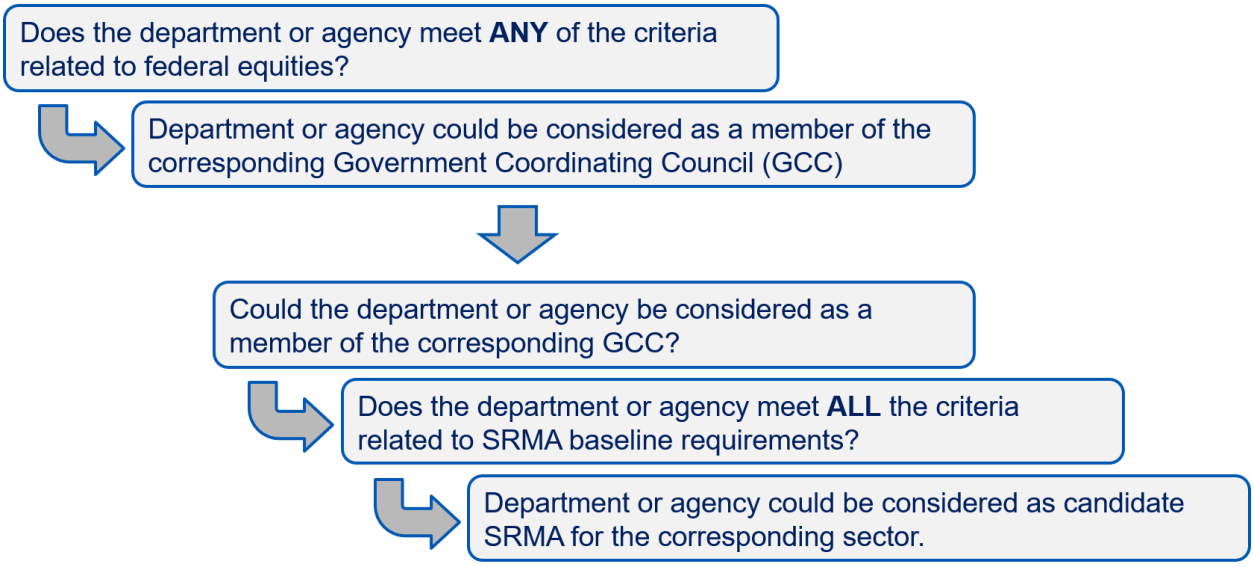


Appendix D: DECISION-SUPPORT FRAMEWORK TO IDENTIFY CANDIDATE SRMAS

Additional criteria must be applied to GCC members when identifying a potential SRMA to chair the GCC. Like the assessment of a potential sector, identifying a potential SRMA answers additional questions that narrows the field for a department or agency to be considered to serve as the SRMA for the corresponding sector.

1. Could the department or agency be considered as a member of the corresponding GCC?
2. Does the department or agency meet all the criteria related to SRMA baseline requirements for responsibilities and capabilities that have not been assumed by owner/operators or local/state agencies? (See Appendix B)

The figure below summarizes the decision process that should guide this evaluation:



In the event multiple GCC members pass the filtering criteria, the agency selected should be the one who can most effectively support the partnership through a combination of:

- technical subject matter expertise,
- trust from the sector to foster and protect information sharing, and
- the ability to resource the SRMA responsibilities.

The ideal SRMA is the department or agency that has the strongest mission-alignment with keeping the sector secure, resilient, and operational while also having the ability to effectively administer SRMA responsibilities.

Appendix E: GLOSSARY OF TERMS

CIPAC	Critical Infrastructure Partnership Advisory Council
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
DoC	Department of Commerce
DOE	Department of Energy
DoI	Department of the Interior
DoT	Department of Transportation
DPP	Domestic Preparedness Program
EO	Executive Order
EPA	Environmental Protection Agency
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
FSLC	Federal Senior Leadership Council
FTE	Full-Time Equivalent
FY	Fiscal Year
GCC	Government Coordinating Council
GSA	General Services Administration
HHS	Department of Health and Human Services
HSPD	Homeland Security Presidential Directive
I&A	Intelligence and Analysis
IC	Intelligence Community
IDT	Infrastructure Data Taxonomy
IPC	Interagency Policy Committee
ISAC	Information Sharing and Analysis Center
ISC	Interagency Security Committee
ISD	Infrastructure Security Division
IT	Information Technology
KIQ	Key Intelligence Question
NCF	National Critical Function
NCD	National Cyber Director
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NSC	National Security Council
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OT	Operational Technology
PCCIP	President's Commission on Critical Infrastructure Protection
PDD	Presidential Decision Directive
PPD	Presidential Policy Decision

R&D	Research and Development
RFA	Request for Assistance
RFI	Request for Information
SCC	Sector Coordinating Council
SLTT	State, Local, Tribal, and Territorial
SRMA	Sector Risk Management Agency
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
THIRA	Threat and Hazard Identification and Risk Assessment
TLP	Traffic Light Protocol
UCG	Unified Coordination Group
USDA	U.S. Department of Agriculture
WMD	Weapon of Mass Destruction