Critical Infrastructure: Emerging Trends and Policy Considerations for Congress

July 8, 2019

Congressional Research Service
https://crsreports.congress.gov
R45809

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

Critical Infrastructure: Emerging Trends and Policy Considerations for Congress

R45809

July 8, 2019

Brian E. Humphreys
Analyst in Science and Technology Policy

Protection of the nation's critical infrastructure (CI) against asymmetric physical or cyber threats emerged in the late 1990s as a policy concern, which was then further amplified by the 9/11 terrorist attacks. Congress created the Department of Homeland Security (DHS) in the wake of the attacks, and directed the new Department to identify, prioritize, and protect systems and assets critical to national security, the economy, and public health or safety. Identification of CI assets was, and remains, a complex and resource-intensive task.

Many governmental and non-governmental stakeholders increasingly advocate for a fundamentally different approach to critical infrastructure security, maintaining that criticality is not a fixed characteristic of given infrastructure assets. Rather, they argue, criticality should be understood in the context of ensuring system-wide resilience of American government, society, and economic life against the full range of natural and manmade hazards.

Congress further elevated resilience as a priority when it passed the Cybersecurity and Infrastructure Security Agency (CISA) Act into law in late 2018. As the name indicates, CISA was created to lead the national cybersecurity and infrastructure security effort as an operational component of DHS. In April 2019, leadership of the new agency identified a set of 56 National Critical Functions (NCF) ("**Appendix A**: National Critical Functions") which it plans to use as the basis of a resilience-based CI risk management approach. However, implementation will rely to a large degree on repurposed legacy programs. Thus, CI policy is currently at an inflection point that raises several potentially pressing issues for Congress:

- Scope of federal CI policy: The CI security enterprise has expanded significantly from its early focus on protecting systems and assets "essential to the minimum operations of the economy and government" against deliberate attack. Congress may consider narrowing the scope of CI policy.
- The legacy policy framework: National CI policy retains many legacy mandates and programs designed to support asset protection despite a long-term policy shift towards an all-hazards resilience framework. Congress may consider revising existing asset identification and reporting requirements statutorily linked to federal homeland security grant award processes.
- Validity of new risk management methods: Congress may assess the potential advantages and drawbacks of the resilience framework, and NCF as the basis for national-level infrastructure risk assessments and investment prioritization. In the past, Congress has called for external validation of DHS risk management methods and may wish to do so in the present case given its comparative novelty.
- Roles and responsibilities of federal agencies: The Homeland Security Act of 2002 created DHS and consolidated many of the federal government's CI security functions in a large-scale reorganization of government and its mission that is still ongoing. Congress may consider transfer of certain infrastructure security related functions to or from DHS as appropriate.
- Scope of regulation: Congress may consider legislating compulsory compliance with security standards in cases where voluntary private-sector measures are deemed insufficient to protect national security, the economy, and public health or safety.
- Appropriateness of existing public-private partnership structures: CISA plans to maintain the current sector specific public-private partnership structures as the preferred vehicle for information sharing and policy coordination. Congress may consider whether adjustment or replacement of these structures is needed to better align partnership efforts with the emerging federal emphasis on system-level resilience.
- Effectiveness of public-private partnerships: CISA and its predecessor organizations have not been able to provide reliable data indicating the reach and effectiveness of public-partnership programs in incentivizing efficient private investments in national level (as opposed to enterprise level) resilience. Congress may consider whether new or revised reporting requirements are necessary.

Contents

Tables

Appendixes

Contacts

Introduction

Critical infrastructure (CI) refers to the machinery, facilities, and information that enable vital functions of governance, public health, and the economy. Adverse events may occur when CI systems and assets are subject to loss or disruption for any cause, whether by natural disasters or deliberate attack.

This report highlights four key areas of enduring policy concern for Congress, and outlines the parameters of ongoing debates within them. A section is devoted below to each key area: defining and identifying CI; understanding and assessing CI risk; federal organization to address CI; and the role of the private sector.

Defining and Identifying CI

Presidential Decision Directive 63 (PDD-63) on critical infrastructure protection, released in 1998, was the first high-level policy guidance for critical infrastructure protection in the contemporary era. It framed the critical infrastructure issue in terms of national vulnerability to potentially devastating asymmetric attacks.[1] The directive presented U.S. military economic and military might as "mutually reinforcing and dependent" elements of national power dependent upon critical infrastructure to function properly.[2] The directive provided an austere definition of critical infrastructure as "those physical and cyber-based systems essential to the minimum operations of the economy and government."[3]

PDD-63 set ambitious national goals for the elimination of any significant national vulnerability to "non-traditional" asymmetric cyber or physical attacks on CI. In practice, it has proven extremely difficult even to establish consistent criteria for assessing the criticality of specific assets and systems, in part because criticality relates not only to the physical attributes of infrastructure systems and assets, but also to the perspectives, values, and priorities of those making the assessment. The sheer scale, complexity, and interconnectedness of the U.S. and global economies complicate efforts to identify and inventory critical assets and systems. For example, the United States electricity sub-sector alone has nearly 7,000 operational power plants, which in turn depend upon other infrastructure assets and complex supply chains to support continuing operations.[4]

The Evolving Definition of CI

The most commonly cited statutory definition of critical infrastructure was established in the USA PATRIOT Act of 2001 (P.L. 107-56), and echoes PDD-63 in its focus on protecting the industrial and demographic foundations of national mobilization against catastrophic risks. The USA PATRIOT Act defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets

[1] Tami Davis Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*, vol. 113 (Princeton, New Jersey: Princeton University Press, 2009).

[2] Presidential Decision Directive 63 (PDD-63), "Critical Infrastructure Protection," p. 1, May 22, 1998.

[3] Ibid., p 1.

[4] Department of Energy, Office of Electricity Delivery and Energy Reliability, *United States Electricity Industry Primer*, DOE/OE-0017, Washington, DC, July 2015, p. 6, at https://www.energy.gov/indianenergy/downloads/united-states-electricity-industry-primer.

would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[5]

Over time, critical infrastructure policy has expanded from its earlier emphasis on the physical foundations of national power to a wider concern with provision of essential services and customary conveniences to the public.[8]

The universe of threats to CI commonly considered by Congress and executive branch departments and agencies has also expanded since the early post-9/11 period.[9] The intelligence community continues to devote significant attention to asymmetric threats to CI posed by state and non-state adversaries who lack the means to directly confront U.S. military power, or for strategic reasons choose to avoid direct military confrontation. Asymmetric attacks may use a combination of physical or cyber means to damage or disrupt domestic CI systems and assets, or cause mass civilian casualties. However, natural disasters and other causes of damage and disruption not directly linked to terrorism or other intentional acts have become more salient elements of critical infrastructure policy and practice in the years since 9/11.

Where Did the Concept of CI Come From?

Awareness of the potential vulnerability of modern infrastructure to deliberate attack or natural disaster dates at least to the interwar era, when American and British military theorists first speculated that targeting the industrial infrastructure and civilian morale of the Axis powers with long-range strategic bombing might bring victory at a comparatively low cost.[6] During World War II, Allied military strategists sought to identify critical vulnerabilities of the Axis industrial base: specific enemy industrial systems and assets, which if destroyed, would pose systemic risk to the Axis war economy.[7] Allied planners faced persistent difficulty in identifying truly critical nodes, and strategic effects of tactically-successful bombing strikes were often mitigated by the system-level resilience of the Axis war economy.

The basic elements of critical infrastructure policy introduced in the late 1990s mirrored the concerns of the wartime planning enterprise in their emphasis on identification and protection of vulnerable critical assets against asymmetric attacks. (Before World War II, strategic bombing was considered a form of asymmetric warfare against countries with large land armies, which the United States lacked at the time.)

Although the USA PATRIOT Act's definition of critical infrastructure remains law and is still commonly cited as a basis for official policy, CI policymakers have lowered the threshold of criticality to include infrastructure-related events with disruptive, but not necessarily catastrophic, effects at all levels of society and government. Policy increasingly reflects local, society-centric perspectives on infrastructure that place emphasis on it as an enabler of prosperity, public safety, and civic life.

For example, National Infrastructure Protection Plan (NIPP), published by DHS in 2013 as official policy guidance for interagency coordination and public-private partnerships, defines

[5] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act §1016(e)

[6] Tami Davis Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing, 1914-1945*, vol. 17. Princeton University Press, 2009.

[7] The concept of critical vulnerabilities has its origins in theories of war pioneered by 19th century Prussian military officer Carl Clausewitz, which have long been part of U.S. military training.

[8] Organization for Economic Cooperation and Development (OECD) (2019), *Good Governance for Critical Infrastructure Resilience, OECD Reviews of Risk Management Policies*, OECD Publishing, Paris.

[9] For discussion of evolution of CI definitions and scope, see Susan Spierre Clark, Thomas P. Seager, and Mikhail V. Chester, "A Capabilities Approach to the Prioritization of Critical Infrastructure," *Environment Systems and Decisions*, vol. 38, 2018, pp. 339–352. Also, CRS Report RL32631, *Critical Infrastructure and Key Assets: Definition and Identification*, by John D. Moteff and Paul W. Parfomak.

critical infrastructure as "assets, systems, and networks that underpin American society," and considers impacts of a wide range of natural and manmade hazard events at the national, regional, and local levels.[10]

Successive Administrations since 1998 have gradually expanded the aperture of CI policy beyond protection of sectors regarded as essential to national security, the economy, and public health and safety. This reflects a global trend among developed countries toward CI policies favoring society-centric resilience at the system level over security-oriented protection of specific assets deemed at risk.

In January 2017, the Department of Homeland Security (DHS) designated U.S. election systems as a sub-sector of the Government Facilities critical infrastructure sector, which also includes national monuments and icons and education facilities.[11] The components of the elections systems as described by DHS include physical locations (storage facilities, polling places, and locations where votes are tabulated) and technology infrastructure (voter registration databases, voting systems, and other technology used to manage elections and to report and validate results).[12] The criticality of these facilities, systems, and assets derives primarily from their essential role in supporting the nation's civic life.

Currently, there are 16 critical infrastructure sectors as set forth in Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," and elaborated in the 2013 NIPP.[13] The federal government uses CI sectors as an organizing framework for voluntary public-private partnerships with self-identified CI owner-operators. Public-private partnership activities are non-regulatory in nature. DHS has overall responsibility for coordination of partnership programs and activities, but in several cases other federal agencies are assigned leading roles as Sector-Specific Agencies (SSAs). (The roles and responsibilities of the public and private sectors are discussed in the final section of this report, "The Role of the Private Sector.") Together, these sectors represent a broad and diverse array of national economic activity and social life, each with its own distinct characteristics.

Table 1. Critical Infrastructure Sectors

CI Sector	Description	Sector Specific Agency
Chemical	Manufactures, stores, transports, or delivers chemicals for industrial use, water treatment, and health.	DHS
Commercial Facilities	Provides venues for business, retail purchases, recreation and lodging.	DHS

[10] U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, Executive Summary, 2013, p. 1. NIPP 2013 supersedes previous plans published in 2009 and 2006, and remains current policy as of this writing.

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

[12] CRS In Focus IF10677, *The Designation of Election Systems as Critical Infrastructure*, by Eric A. Fischer.

[13] Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," February 12, 2013, at https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil. (Supersedes Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," December 17, 2003.) By contrast, PDD-63, released in 1998, focused on functions that are now contained within designated lifeline sectors of Communications, Energy, Transportation Systems, and Water and Wastewater systems, with the exception of emergency law enforcement and "continuity of government" services. See PDD-63, Annex A, op. cit., p. 10.

CI Sector	Description	Sector Specific Agency
Communications	Provides wired, wireless, and satellite communications to meet the needs of businesses and governments.	DHS
Critical Manufacturing	Processes raw materials and produces highly specialized parts and equipment essential to primary operations in U.S. industries—particularly transportation, defense, electricity, and construction.	DHS
Dams	Manages water retention structures, including levees, dams, navigation locks, canals (excluding channels), and nationally symbolic hydroelectric dams.	DHS
Defense Industrial Base	Supports military operations; performs R&D; design, manufactures, and integrates systems; and maintains depots and services military weapon systems, subsystems, components, subcomponents, or parts.	Department of Defense
Emergency Services	Provides fire, rescue, emergency medical services, and law enforcement.	DHS
Energy	Provides the electric power used by all sectors and the refining, storage, and distribution of oil and gas. The sector is divided into electricity, and oil and natural gas.	Department of Energy
Financial Services	Provides critical financial utilities and services that support investment, credit and financing, and insurance.	Department of Treasury
Food and Agriculture	Produces, processes, distributes, and serves food.	Department of Agriculture
Government Facilities	Includes a wide variety of nearly 900,000 constructed assets owned or leased by Federal, State, local, tribal, or territorial governments, used to provide the full range of government services.	DHS and Government Services Administration
Healthcare and Public Health	Provides essential healthcare and public health services. Conducts related research and development; manufactures pharmaceuticals and other essential medical supplies; and manages supply chains required for care delivery.	Health and Human Services
Information Technology	Produces information technology and incudes hardware manufacturers, software developers, and service providers, as well as the Internet as a key resource.	DHS
Nuclear Reactors, Materials, and Waste	Provides nuclear power and materials used in a range of settings. Includes commercial and research reactors, fuel fabrication facilities, reactor decommissioning, and the transportation, storage, and disposal of nuclear materials and waste.	DHS
Transportation Systems	Enables movement of people and assets with the use of aviation, ships, rail, pipelines, highways, trucks, busses, and mass transit	DHS and Department of Transportation
Water and Wastewater Systems	Provides drinking water and treatment of wastewater.	Environmental Protection Agency

Sources: NIPP 2013, Sector-Specific Plans, and GAO-18-211.

The expanding multiplicity and breadth of definitions used for critical infrastructure designation has policy implications for Congress. Each officially-designated critical infrastructure sector is represented by formal coordination bodies, which include numerous private sector stakeholder groups and representatives of state, local, tribal, and territorial (SLTT) governments. In addition, industry and non-profit groups may participate in certain sector-wide activities. As sectors

mature, new public and private sector communities of interest emerge within the broader critical infrastructure enterprise, each with its own unique perspective on what criticality means as applied to the nation's infrastructure.

For this reason, there is no single, consistently applied definition of critical infrastructure. Even though the most commonly cited statutory definition of CI has not changed in nearly two decades, identification and prioritization of critical systems and assets as categories of applied practice reflects diverse interests and perspectives, which continue to evolve. This suggests that definitions of critical infrastructure are not merely a matter of semantics, and the multiplicity of official definitions in common use is not simply a matter of imprecision. Rather, variation reflects diverse constituencies' efforts to negotiate the boundaries of congressional responsibility, the scope of government programs, and the nature and extent of public-private sector relationships at any given point in time.

CI Protection vs. CI Resilience

Critical infrastructure policy has taken on two distinct orientations that significantly overlap but nonetheless reflect different organizational perspectives and requirements. Critical infrastructure protection (CIP) emphasizes the identification, prioritization, and protection of infrastructure assets. Criticality from this perspective is generally defined in terms of the consequences of asset loss or system disruption (i.e., an infrastructure asset or system is critical to the degree that loss or disruption of service would have system-level impacts on essential functions of society, the economy, or government). Critical infrastructure resilience (CIR) emphasizes broad investments in hazard mitigation and preparedness during steady-state periods, and adaptation during emergencies, to ensure availability of critical infrastructure functions that enable provision of essential services.

Much of the major legislation that serves as the foundation for CI policy was passed in the immediate aftermath of the 9/11 attacks, when concerns with physical protection of critical assets predominated in policy circles. However, policy practice in the United States and other developed countries has increasingly favored a focus on system resilience over asset protection. As such, national CI policy reflects a hybrid approach that contains elements of both CIP and CIR. This can exacerbate already complex issues inherent in defining criticality and identifying what exactly is critical in the context of time and place. Recognizing this inherent tension, this report uses the term "critical infrastructure security" to discuss CI policy without favoring CIP or CIR.

CIP Asset Lists, Catalogs, Databases, and Reports

CIP-focused legislation and government policy directives since 2001 have frequently contained requirements for the creation of asset lists, catalogs, databases, and reports to identify systems and assets that meet a given threshold of criticality, and thus require higher than ordinary levels of protection against plausible threats. The logic is simple on its face: we need to know what we have; what is most important; and what we need to protect.

However, application of this logic often introduces many complexities in actual practice, and so national-level issues of asset identification and prioritization persist across all CI sectors. Nonetheless, inventory requirements are typically the first step of the broader risk management strategies applied to critical infrastructure protection, both at the national level and in the private sector at the enterprise level. Definitional criteria of criticality will likely continue to be a subject of considerable debate within the CI policy community, but the forcing mechanism provided by list/no-list decisions serve to define what specific assets are considered critical in actual practice.

Policy Guidance for Asset Identification

One of the earliest examples of a CIP-based inventory requirement is the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, released in February 2003 just before the newly created Department of Homeland Security began operations. The strategy directed DHS to develop a "uniform methodology for identifying facilities, systems, and functions with national-level criticality," and use it to "build a comprehensive database to catalog these critical facilities, systems, and functions."[14]

It was followed by the December 2003 release of *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* (HSPD-7), which served as the basis of CI policy development and implementation for the next decade until it was superseded by PPD-21 in 2013. HSPD-7 shared the CIP-orientation of other early policy documents, directing federal departments and agencies to "identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them."[15] DHS claimed in the 2006 NIPP—the first plan of its type—that it had compiled a comprehensive CI database to meet the CI identification requirement.[16]

However, a 2006 DHS Inspector General (IG) report found that these early efforts to produce a national database of CI assets suffered from conceptual and methodological shortcomings.[17] The report stated that the Department's National Asset Database had rapidly grown from 160 key assets in 2003 to include 77,069 assets in 2006, and that listed assets included everything from nuclear power plants and dams to local petting zoos and water parks. The IG report concluded that the database contained many entries that listed "unusual, or out-of-place, assets whose criticality is not readily apparent," without providing assurance that truly critical assets *were* included.[18] Likewise, data collection procedures were not standardized, so that San Francisco listed its entire light rail system as a single asset, while New York City listed its subway stations as multiple individual assets.

Congressional Oversight of Asset Identification

Congress subsequently included provisions for the National Asset Database as part of the Implementing the Recommendations of the 9-11 Commission Act of 2007 (P.L. 110-53, The 9-11 Commission Act). The legislation requires compilation of a national database of vital systems or assets, and creation of a separate classified list of "prioritized critical infrastructure," to be updated annually and submitted to Congress. The classified list is to include assets that the Secretary determined would cause national or regional catastrophic effects if subject to disruption or destruction. Other provisions include definitions of infrastructure-related terms, and a requirement for the Secretary to implement certain quality control procedures to ensure that asset

[14] The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, Planning and Resource Allocation*, February 2003, p. 23.

[15] The White House, *Homeland Security Presidential Directive 7*, at https://www.dhs.gov/homeland-security-presidential-directive-7.

[16] U.S. Department of Homeland Security, *National Infrastructure Protection Plan 2006*, 2006, p. 31.

[17] U.S. Department of Homeland Security, Office of the Inspector General, *Progress in Developing the National Asset Database*, June 2006.

[18] Ibid., p. 9.

nominations from state governments or other sources meet the threshold of criticality as determined by the Secretary.[19]

A 2013 Government Accountability Office (GAO) report found that DHS had improved its processes for critical asset identification, but that significant questions regarding reporting criteria and methodology persisted.[20] The report documented frequent changes in nomination and adjudication criteria and reporting format used by National Critical Infrastructure Prioritization Program (NCIPP), which DHS instituted to fulfil the congressional mandate of the 9-11 Commission Act. After 2009, NCIPP assessed criticality of all nominations according to four types of potential adverse consequences above certain designated thresholds: fatalities, economic loss, mass evacuation length, and national security impacts.[21]

Methodological adjustments were subsequently made in some cases to account for unique CI characteristics. For example, collapse of the U.S. financial system would likely not cause immediate mass casualties, but might still have debilitating second-order effects on national security, economic security, and public health and safety.[22] The same might also apply to election infrastructure used in federal elections, which was added as a CI sub-sector in 2017. The report noted that asset nomination vetting methods had not undergone an independent peer review. It recommended to Congress that DHS commission such a review to "assure that the NCIPP list identifies the nation's highest priority infrastructure."[23]

Policy and Legal Implications of Criticality Designation

Being listed as a prioritized asset in the NCIPP immediately elevates a given asset making it an object of national significance under relevant statutes. This action may affect government prioritization of certain on-site risk assessments, administration of regulatory regimes and grant programs, conduct of certain criminal prosecutions, and emergency preparedness and response coordination, among other activities. Exact numbers of nominated assets are not publicly available due to classification requirements, but they number in the thousands.[24]

Despite the often significant ramifications of the NCIPP list, the 2013 GAO report found that some state governments were opting not to participate in DHS data calls, citing compliance burdens, technical limitations, and cost-benefit calculations.[25] For example, some states said they lacked expertise to develop scenarios and model complex infrastructure systems with sufficient fidelity to assess likely consequences of failure or disruption.[26] For this reason alone, the NCIPP list cannot be regarded as a current and complete national inventory of critical systems and assets. Furthermore, GAO found that DHS was unable to provide documentation to show that it had complied with the statutory annual reporting requirement in recent years. The inherent

[19] P.L. 110-53.

[20] U.S Government Accountability Office, *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, GAO-13-296, March 2013.

[21] Ibid,, p. 13. Previously, criticality was based on measures of capacity, such as commercial facility occupancy limits, throughput of pipeline, etc.

[22] Ibid., pp. 15-16.

[23] Ibid., p. 1. In November 2013, DHS commissioned a panel for this purpose, according to testimony provided to Congress. See U.S. Government Accountability Office, *Critical Infrastructure Protection: DHS Has Made Progress in Enhancing Critical Infrastructure Assessments, but Additional Improvements Are Needed*, GAO-16-791T, July 2016, p. 14.

[24] Ibid., p. 9.

[25] Ibid., pp. 30-31.

[26] Ibid., p. 30.

complexities of CI inventory and categorization as described above also suggest the presence of persistent difficulties in assuring the completeness, quality, and currency of centralized inventories of CI assets requiring protected status.

CIR Identification of Systems and Assets

CIR prioritizes adaptive use of critical capabilities to enable continuity of service during periods of stress on critical infrastructure systems. This approach to CI inventory expands the scope of data collection to include any and all assets within a given CI sector that might be useful in emergency planning or contingency situations—regardless of their inclusion on a particular list. The data can then be used as needed to identify alternative means of maintaining critical functions and providing essential services if systems and assets ordinarily used to provide these services are compromised.

The major CI interagency database using the capabilities approach is known as Homeland Infrastructure Foundation–Level Data (HIFLD). Four lead agencies—DHS, Department of Defense (DOD), the National Geospatial-Intelligence Agency, and the U.S. Geological Survey—compile data gleaned from outreach to public and private sector partners, and make it available to eligible law enforcement, emergency management, and other organizations at all levels of government.[27]

HIFLD is comprised of hundreds of data "layers," which encompass nearly every conceivable category of asset relevant to homeland security functions and are curated by designated partner agencies, or "stewards" as they are known.[28] Layers include assets considered critical under any definition, which are essential to supporting lifeline CI functions of energy, communications, transportation systems, and water and wastewater systems.[29] However, HIFLD also includes many asset categories that are not necessarily critical according to any given statutory or official definition of criticality, but may *become* critical in the context of specific emergencies or CI policy decisions—for example, truck driving schools, express shipping facilities, and cruise ship terminals.

The Department of Health and Human Services (HHS) used HIFLD during the 2017 hurricane season to locate day care centers in impacted areas.[30] These specific day care centers would likely not be defined as critical under the common statutory definition of CI, because they were not so vital to the functioning of the national public health system as a whole that physical loss of the facilities would be debilitating at the national level. However, knowledge of where these centers were located was essential in allowing HHS to provide a critical public health service—ensuring the safety of children in a disaster zone.

The HIFLD partnership model is intended to enable relevant agencies at all levels of government and certain private sector entities to leverage a large universe of readily-accessible infrastructure data to address real-world use cases. Unlike the NCIPP list, it does not elevate the status of specific systems and assets in ways that directly support official functions of federal oversight,

[27] U.S. Department of Homeland Security, "About HIFLD," at https://gii.dhs.gov/hifld/content/about-hifld.

[28] Homeland Infrastructure Foundation-Level Data Subcommittee, "HIFLD Secure," at https://gii.dhs.gov/hifld/data/secure/.

[29] NIPP 2013 identifies communications, energy, transportation, and water as "lifeline functions that are essential to the operation of most critical infrastructure sectors." See NIPP 2013, ibid., p. 17.

[30] Homeland Infrastructure Foundation-Level Data Subcommittee, "HILFD Use Cases—2018," p. 3, at https://gii.dhs.gov/hifld/node/1400.

regulation, and administration. However, it is widely used to inform preparedness and incident management activities of federal and SLTT agencies.

The robust development of HIFLD partnerships at all levels of government in recent years contrasts with the declining state participation in NCIPP documented by GAO. Nonetheless, CIP-based approaches to inventory of CI assets remain relevant. For example, provisions of the 2017 National Defense Authorization Act related to national preparedness against electromagnetic threats and hazards required DHS to determine, to the extent practicable, "the critical utilities and national security assets and infrastructure that are at risk.... "[31] Likewise, specific chemical manufacturing facilities posing a high risk for malicious exploitation continue to be subject to DHS inspection and regulatory enforcement under Chemical Facility Anti-Terrorism Standards (CFATS) first authorized by Congress in 2007.[32] These regulations require owner-operators to protect their facilities against cyber and physical threats according to specified standards.

Issues for Congress

Congress may consider the implications of the policy shift towards system-level resilience for legacy programs, such as the NCIPP asset list. Continuing policy changes made by DHS may further reduce the profile of NCIPP specifically, and asset-protection approaches to CI risk management in general. Stakeholder participation in NCIPP is not cost-neutral, so Congress may consider the frequency of data calls, elimination of any overlapping efforts or duplication, or additional appropriations to support data gathering and analysis. Congress may also consider updates to National Asset Database requirements contained in the 9/11 Commission Act to ensure their continuing relevance and applicability to emerging CISA programs and priorities, and their alignment with the requirements of other congressionally authorized programs, such as the Homeland Security Grant Program.

Understanding and Assessing CI Risk

Efforts to identify and prioritize CI systems and assets are part of a larger national effort to systematically understand and assess homeland security risks. In recent decades, Congress has frequently sought authoritative assessments of national level risk to CI. Risk assessments may be used to inform planning and resource allocation decisions related to congressional appropriations, emergency preparedness, regulatory oversight of certain industries, federal grant funding, and voluntary security measures by CI owner-operators.

DHS, which is responsible for coordination and oversight of the national infrastructure security effort, defines risk as the "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences."[33] DHS officially considers three factors as components of risk: threat, vulnerability, and consequence.

[31] P.L. 114-328. Section 1913(a)(i) states, "Within 90 days of the date of this order, the Secretary of Homeland Security, in coordination with the heads of SSAs and other agencies as appropriate, shall identify and list the national critical functions and associated priority critical infrastructure systems, networks, and assets, including space-based assets that, if disrupted, could reasonably result in catastrophic national or regional effects on public health or safety, economic security, or national security.... " Also see Executive Order 13865, "Coordinating National Resilience to Electromagnetic Pulses," 84 *Federal Register* 12041, March 26, 2019.

[32] See CRS In Focus IF10853, *Chemical Facility Anti-Terrorism Standards*, by Frank Gottron.

[33] U.S. Department of Homeland Security, *DHS Risk Lexicon*, Washington, DC, September 2010, p. 27, at https://www.dhs.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf.

DHS defines threat as "a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property."[34] Threat assessments usually include data on human adversaries or natural hazards, such as extreme weather events. In the case of the former, threat estimates are based on available information about the identity of threat actors or groups, and their motivations, capabilities, and observed targets. Information on likely timing, methods, and frequency of attacks may also be incorporated if available. In the case of natural hazards, likelihood and severity of event occurrence is usually estimated using databases of past similar events in conjunction with predictive modeling of weather, tectonic activity, and the like.

DHS defines vulnerability as the "physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard."[35] Vulnerability assessments provide information about characteristics of assets or systems that may leave them open to exploitation or damage from a threat or hazard. This may include, for example, software design characteristics or structural weaknesses in a levy system. Assessments may contain recommendations for adoption of resilience measures to mitigate identified vulnerabilities.[36]

DHS defines consequence as the "effect of an event, incident, or occurrence."[37] As discussed in the previous section, criticality assessments focus on potential consequences of adverse events that disrupt or destroy infrastructure systems and assets. These assessments use a range of technical and non-technical methods of assessment. Research centers, universities, and industry groups develop and refine many different modeling methodologies to inform infrastructure security investments and activities of federal agencies and SLTT jurisdictions. In other cases, recognized subject-matter experts and responsible officials make non-technical assessments based upon accumulated knowledge and experience. Consequence-based criticality assessments can be used to inform risk assessments when combined with threat and vulnerability assessments.

Since 2007, DHS has applied these elements of risk to its various planning, programs, and budget activities as a function: "risk is a function of threat, vulnerability, and consequence," or R=f(TVC).[38] Critics have challenged the usefulness of this formula on several grounds. They assert DHS has not demonstrated the capability to accurately assign probabilities to rare events like terrorist attacks, or otherwise determine precise values for all the terms in the equation. Likewise, the terms of the equation are not necessarily independent from one another. Complex interactions between threat, vulnerability, and predicted consequences make application of this formula to grant applications and other resource allocation decisions related to risk mitigation problematic.[39]

---

[34] Ibid., p. 36.

[35] Ibid., p. 38.

[36] For example, see U.S. Department of Energy, *Climate Change and the U.S. Energy Sector: Regional Energy Sector Vulnerabilities and Resilience Solutions*, 2015, at https://www.energy.gov/maps/regional-climate-vulnerabilities-and-resilience-solutions.

[37] U.S. Department of Homeland Security, *DHS Risk Lexicon*, op. cit., p. 10.

[38] See CRS Report RL33858, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, by Todd Masse, Siobhan O'Neil, and John W. Rollins; also see Government Accountability Office, "Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure," GAO 06-91, December 2005, p. 111.

[39] CRS Report RL33858, *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, by Todd Masse, Siobhan O'Neil, and John W. Rollins. Also see National Research Council, Review of the Department of Homeland Security's Approach to Risk Analysis (Washington, DC: The National

DHS recognized in 2018 the need to provide a "complete systemic risk picture" for CI, and has proposed revision or updates to risk assessment approaches described above.[40] Several significant legislative and executive branch initiatives related to CI risk assessment were instituted in 2018-2019 to establish the organizational basis for significant changes. The Cybersecurity and Infrastructure Security Agency Act of 2018 (CISA Act; P.L. 115-278) created the eponymous agency (CISA) as an operational component of DHS to take over the functions previously carried out by the National Protection and Programs Directorate (NPPD) as a DHS headquarters organization.[41]

The creation of a dedicated agency for infrastructure security elevates CI risk management as an area of policy focus. CISA has established the National Risk Management Center (NRMC) as a "planning, analysis, and collaboration center" to manage national CI risk.[42] According to CISA, the NRMC will adopt an "evolved approach" to CI risk management, which emphasizes cross-sector analysis, and capabilities-oriented approaches to identification and prioritization of CI.[43]

Issues for Congress

Congress may request information from CISA on its efforts to institutionalize new risk management methods and approaches, and to ensure that these are validated by qualified external reviewers. The National Laboratories, the relevant university-based DHS Centers of Excellence, certain other universities and research centers, industry research groups, and the Homeland Security Advisory Council may provide relevant expertise in infrastructure risk assessment methodology. The Homeland Security Act specifies how the Secretary of Homeland Security may leverage these organizational resources in support of homeland security activities. Congress may choose to exercise its discretion in establishing funding priorities and program guidance for these organizations as appropriate to support national CI security goals.

Federal Organization to Address CI

Federal organization to address CI issues has changed significantly in response to evolving threats and the accompanying maturation of the homeland security enterprise. Three distinct periods of development are covered below: the initial policy development and coordination initiatives of the late 1990s; the post-9/11 reorganization of federal government to counter terrorist threats to infrastructure; and the ongoing transition to the all-hazards resilience framework for infrastructure security.

Academies Press, 2010), p. 52. The relevant passage reads, "... the committee concludes that Risk = T × V × C is not an adequate calculation tool for estimating risk in the terrorism domain, for which independence of threats, vulnerabilities, and consequences does not typically hold and feedbacks exist." See also Louis Anthony Cox, Jr., "Some Limitations of 'Risk=Threat×Vulnerability×Consequence' for Risk Analysis of Terrorist Attacks," Risk Analysis: An International Journal, vol. 28, no. 6, 2008, p. 1753.

[40] U.S. Department of Homeland Security, *DHS National Cybersecurity Summit: Protecting Critical National Functions through Industry and Government Collaboration*, Fact Sheet, Washington, DC, July 31, 2018, p. 2, at https://www.dhs.gov/sites/default/files/publications/18_0731_cyber-summit-national-cybersecurity-summit-fact-sheet.pdf.

[41] The Cybersecurity and Infrastructure Security Agency Act of 2018 (P.L. 115-278).

[42] CISA, "National Risk Management," at https://www.dhs.gov/cisa/national-risk-management.

[43] CISA, "National Critical Functions," at https://www.dhs.gov/cisa/national-critical-functions.

From the 1990s to the Homeland Security Act

Federal attention to CI policy increased in the 1990s as concerns grew about the potential for malicious exploitation of the expanding interface between computing technologies and physical infrastructure. The Clinton Administration established the Commission on Critical Infrastructure Protection in 1996 with a mandate to produce a report on infrastructures "that constitute the life support systems" of the nation, with a focus on emerging cyber threats.[44] Two years later the Administration issued PDD-63 based in part on the Commission's report, requiring the government "to swiftly eliminate any significant vulnerability" of critical infrastructures to "non-traditional" cyber or physical attack within five years.

The organizational directives set forth in PDD-63 focused on increasing interagency coordination by leveraging existing federal entities. The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, the senior executive position created by the directive, did not report directly to the President, and his duties were confined largely to leadership of an interagency coordination group and service as executive director of a stakeholder advisory group.

Congress chartered a blue ribbon commission in 1999 to assess both terrorist threats to national security and early efforts to implement PDD-63. The Gilmore Commission, as it was known, submitted a report to Congress and the White House in December of 2000 titled "Toward a National Strategy for Combating Terrorism." The report found that implementation of PDD-63 was incomplete, and that the nascent CIP enterprise had developed only fitfully since it was signed in 1998.[45] Specifically, it found

- Information Sharing and Analysis Centers (ISACs) created to facilitate broader risk awareness in government and industry about infrastructure vulnerabilities and threats were "still embryonic."
- The National Coordinator for Security, Infrastructure Protection, and Counterterrorism had broad authorities that left little time for CIP responsibilities, and lacked program and budget authority.
- No overall national CIP strategy existed to guide government actions.
- The National Infrastructure Protection Center (NIPC), responsible for CI threat and vulnerability assessments, warning and response coordination, and law enforcement investigation and response activities, had taken few concrete actions to establish its basic functions under Federal Bureau of Investigation (FBI) auspices.

Consolidation and the Creation of DHS

The 9/11 attacks had a galvanizing effect on homeland security policy, and, by extension, critical infrastructure protection. Policy initiatives that had previously languished became matters of

[44] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, The Report of the President's Commission on Critical Infrastructure Protection, Washington, DC, October 1997, p. i.

[45] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Toward a National Strategy for Combating Terrorism*, Second Annual Report, Arlington, VA, December 15, 2000, at https://www.rand.org/content/dam/rand/www/external/nsrd/terrpanel/terror2.pdf. The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, known as the Gilmore Commission after its chairman, Virginia governor James S. Gilmore III, was established by Section 1405 of the National Defense Authorization Act for Fiscal Year 1999 (P.L. 105-261).

urgent national concern overnight. Two broad tracks of legislative action emerged. The first favored reestablishing the Office of Homeland Security and the national coordination role under statute, with the addition of certain budget authorities, responsibilities, and oversight requirements, similar in organization and scope to the National Office of Drug Control Policy.[46] This option followed the recommendations of the Gilmore Commission, and would have left much of the existing federal government structure intact, focusing on improved interagency coordination to ensure increased protection against major terrorist attacks.

The second legislative track favored comprehensive consolidation of government counterterrorism functions under a single federal agency to be named the National Homeland Security Agency. This track followed the recommendations of a blue ribbon panel chartered by DOD in 1998 to study 21st century security issues, known as the Hart-Rudman Commission.[47] Key supporters in Congress believed that dispersion of homeland security-related functions across federal departments and agencies whose missions were not primarily security related had left the nation vulnerable to terrorist attacks. They favored consolidation to ensure clearer lines of executive authority, centralization of relevant counterterrorism functions, and better interagency coordination, among other anticipated benefits. The Homeland Security Act of 2002 generally reflected the approach that the Hart-Rudman Commission had advocated for.

The Homeland Security Act P.L. 107-296 transferred many infrastructure security functions to DHS—functions which previously had been regarded as properly belonging to the various diverse spheres of business, finance, commerce, energy, public health, agriculture, and environmental protection. GAO designated creation of DHS as high risk in 2003 because of the large number of agencies being transferred, and the management challenges this presented to the new department.[48] DHS ultimately incorporated nearly three dozen federal agencies and other entities into four major directorates: Information Analysis and Infrastructure Protection, Science and Technology, Border and Transportation Security, and Emergency Preparedness and Response.[49] Although several long-established agencies such as the Coast Guard retained customary missions not related to homeland security, the new departmental structure prioritized their homeland security related missions, especially counterterrorism.

Policy and Budgetary Implications of Organizational Change

This approach represented a change from what infrastructure policy had previously been. The White House had regarded CIP as only tangentially related to counterterrorism functions of government before 9/11. The Office of Management and Budget (OMB) stated in a report to Congress on federal counterterrorism programs, submitted in August 2001, that "CIP is a *separate* but related mission."[50] The authors justified this distinction on the grounds that infrastructure risks were diverse, and included many hazards beyond terrorism to include equipment failure,

[46] See Charles R. Wise, "Organizing for Homeland Security," *Public Administration Review*, vol. 62, no. 2 (March/April 2002), pp. 135-136.

[47] Formally known as the U.S. Commission on National Security/21st Century, the Commission was commonly referred to the Hart-Rudman Commission after its chairmen, former Senators Gary Hart and Warren Rudman.

[48] U.S. Government Accountability Office, "DHS Management—High Risk Issue," at https://www.gao.gov/key_issues/dhs_implementation_and_transformation/issue_summary#t=0. Also see U.S. Government Accountability Office, *Homeland Security: Title III of the Homeland Security Act of 2002*, GAO-02-927T, July 9, 2002, at https://www.gao.gov/assets/110/109473.pdf.

[49] NIPC was among the many entities transferred.

[50] White House Office of Budget and Management, *Annual Report to Congress on Combating Terrorism*, August, 2001, p. 2. (Original emphasis.)

human error, weather and natural disasters, and criminal activity. They wrote, "This year's report focuses on combating terrorism, mentioning CIP efforts only where they directly impact the combating terrorism mission."[51] That direct impact, according to budget estimates in the 2001 report, was negligible. CIP funding that overlapped counterterrorism amounted to less than half of one percent of the total CIP funding of $2.6 billion requested by the White House for the 2002 fiscal year.[52]

9/11 changed the budget picture significantly, as seen in the 2003 OMB report to Congress.[53] Infrastructure programs and activities that had not previously been seen as directly impacting the combating terrorism mission were included in the report, and their relation to counterterrorism efforts highlighted.

Requested budget increases for FY2004 reflected the newfound centrality of counterterrorism priorities across federal departments and agencies with infrastructure-related programs. The White House request for FY2004 was $12.1 billion, representing an increase of more than 450% over its final pre-9/11 request, and included 28 federal entities outside the newly-created DHS. The 2003 report did not provide a separate estimate of the proportion of the CIP-related budget that overlapped counterterrorism, as the 2001 report had. This was hardly necessary in any case, because CIP in all its diverse aspects had largely been redefined as a counterterrorism mission.[54]

Evolution of CI Policy Since the Establishment of DHS

Creation of a new purpose-built department was intended to ensure that CIP and other core homeland security missions were institutionalized as top federal priorities under unified leadership.[55] Under the new consolidation of functions, more than half of the government's pre-9/11 homeland security funding was transferred to a single agency.[56] However, the amalgam of independent agencies transferred to DHS retained significant independence as operational components of the new Department. Likewise, other departments and agencies outside DHS retained many of the infrastructure security functions they had before 9/11. Therefore, despite significant changes, CIP remains a highly distributed enterprise that competes for limited resources with other priorities across the federal government.

Perceived Threat of Terrorism and CIP Priorities

As long as the threat of terrorism continued to be an overriding national priority, counterterrorism continued to be a focal point for critical infrastructure security policy. However, by the time Hurricane Katrina struck the Gulf Coast in August 2005, nearly four years after the 9/11 attacks, public perception of the terrorist threat had already softened considerably. In the immediate aftermath of the attacks, 46% of Americans surveyed by Gallup named terrorism as the most

[51] Ibid., p. 6. According to OMB budget estimates in the 2001 report, CIP funding that overlapped terrorism amounted to less than half of one percent of the total CIP funding of $2.6 billion across the federal government.

[52] Ibid.

[53] White House Office of Budget and Management, 2003, op. cit.

[54] OMB 2001, op. cit., p. 37.

[55] Senator Joe Lieberman, "Letter to Homeland Security Advisor Tom Ridge," March 19, 2002, at https://www.hsgac.senate.gov/media/majority-media/lieberman-seeks-answers-from-ridge-on-homeland-security-improvements. Senator Lieberman served as Chairman of the Senate Government Affairs Committee and introduced legislation to create a National Department of Homeland Security. Also see The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Letter from the President, February 2003.

[56] OMB 2003, op. cit., p. 7.

important problem facing the United States. By the second half of 2005, the percentage hovered between 6%-8%.[57] This broad trend has continued, with periodic upticks caused by high-profile incidents. Gallup surveys in early 2019 did not list terrorism as a category of public concern, because it did not garner sufficient responses to be included in results.[58]

After Katrina, the well-publicized failure of the extensive levy system designed to protect New Orleans from catastrophic floods further highlighted the vulnerability of critical systems and assets to diverse hazards besides terrorism. Issues of equipment failure, human error, weather and natural disasters, and criminal activity highlighted in the pre-9/11 OMB report (described above) reemerged as national-level policy concerns.

New Strategic Directions

In 2006, the Critical Infrastructure Task Force of the Homeland Security Advisory Council initiated a public policy debate arguing that the government's critical infrastructure policies were focused too much on protecting assets from terrorist attacks and not focused enough on improving the resilience of assets against a variety of threats. According to the Task Force, such a defensive posture was "brittle." Not all possible targets could be protected and adversaries could find ways to defeat defenses, still leaving the nation having to deal with the consequences.[59] In 2008, as part of its oversight function, the House Committee on Homeland Security held a series of hearings addressing resilience. At those hearings, DHS officials argued that government policies and actions did encourage resilience as well as protection.[60] Even so, subsequent policy documents made greater reference to resilience.

The 2010 Quadrennial Homeland Security Review (QHSR), the first top-level DHS strategic review submitted to Congress under Title VII of the Homeland Security Act, highlighted the diversity of missions and stakeholders in what had become an expansive enterprise.[61] The QHSR stated that, "while the importance of preventing another terrorist attack in the United States remains undiminished, much has been learned since September 11, 2001, about the range of challenges we face."[62] Examples of threats and hazards included natural disasters (specifically, Hurricane Katrina), widespread international cyberattacks, the expansion of transnational criminal activities, and contagious diseases.

The QHSR noted the leadership role of DHS in managing risks to critical infrastructure, as well as other homeland security missions related to immigration, border security, cybersecurity, and disaster response. However, it presented homeland security as a decentralized enterprise shared

[57] Jim Norman, "How High Will Terrorism Concerns Rise, How Long Will They Last?" *Gallup*, June 15, 2016, at https://news.gallup.com/poll/192713/high-terrorism-concerns-rise-long-last.aspx.

[58] Gallup, "In Depth: Topics A to Z: Most Important Problem," at https://news.gallup.com/poll/1675/most-important-problem.aspx, May 8, 2019.

[59] Homeland Security Advisory Council, *Report of the Critical Infrastructure Task Force*, Washington, DC, January 2006, p. 4.

[60] U.S. Congress, House Committee on Homeland Security, *Partnering with the Private Sector to Secure Critical Infrastructure: Has the Department of Homeland Security Abandoned the Resilience-Based Approach?*, 110th Cong., 2nd sess., May 14, 2008, Serial No. 110-114, p. 7.

[61] P.L. 107-296

[62] U.S. Department of Homeland Security, *Quadrennial Homeland Security Review Report*, Executive Summary, February, 2010, p. i. See P.L. 107-296 as amended by P.L. 115-387, Sec. 707.

by diverse stakeholders in the public and private sector. "[A]s a distributed system," the report read, "no single entity is responsible for or directly manages all aspects of the enterprise."[63]

In 2013, PPD-21 superseded HSPD-7, which had provided authoritative policy guidance for federal infrastructure protection for a decade. PPD-21, which remains in force, informed development of the 2013 NIPP. It placed less emphasis protection of physical infrastructure assets against terrorist threats than HSPD-7 did. Rather, it emphasized all-hazards CI resilience as part of a broader national disaster preparedness effort. "Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards," it stated. "Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery."[64]

The 2014 QHSR further expanded the boundaries of critical infrastructure security beyond terrorism-related threats to include factors such as aging and neglect of critical systems and assets—recasting once-ordinary issues of investment, maintenance, and utility service provision as homeland security concerns.[65] DHS did not submit a QHSR to Congress in 2017 as required by the Homeland Security Act.[66] This means there is no current departmental-level statement that specifies DHS strategic direction and priorities for infrastructure security or other homeland security goals.

The boundaries of responsibility for critical infrastructure security—as well as the definition of critical infrastructure itself—continue to be negotiated among Congress, executive branch departments and agencies, SLTT jurisdictions, and a diverse array of private-sector stakeholders. For example, in 2002 Congress directed the U.S. Department of Agriculture (USDA) to transfer the Plum Island Animal Disease Center to DHS under the Homeland Security Act (P.L. 107-296), based partly on concerns that terrorists might target the nation's food and agriculture sector with contagious pathogens. However, in 2018 Congress authorized transfer of a replacement facility and its functions back to USDA from the DHS Science and Technology Directorate under the Consolidated Appropriations Act of 2018 (P.L. 115-141), as proposed by the White House in its FY2019 budget request.[67] After a relatively brief period of extensive consolidation in the early 2000s, critical infrastructure security in the federal government has evolved into a distributed enterprise loosely structured by institutionalized partnerships and policy frameworks that increasingly emphasize an all-hazards approach to critical infrastructure security.

Issues for Congress

Congress may consider which aspects of critical infrastructure security properly reside within the homeland security enterprise, and which relate more closely to government responsibilities in

[63] U.S. Department of Homeland Security, *Quadrennial Homeland Security Review Report, Executive Summary*, February 2010, p. 13.

[64] PPD-21, "Introduction," op. cit.

[65] For example, the 2014 QHSR cited the 2010 Deepwater Horizon oil spill—an industrial accident caused in part by negligence—as a homeland security hazard. See U.S. Department of Homeland Security, *Quadrennial Homeland Security Review Report*, Executive Summary, February 2014, p. 5.

[66] P.L. 110-53 (6 U.S.C. 347). According to statute, the QHSR must be submitted "not later than December 31 of the year in which a quadrennial homeland security review is conducted." Reviews were required every four years beginning in 2009.

[67] U.S. Department of Agriculture, *Memorandum of Agreement Between the U.S. Department of Agriculture Marketing and Regulatory Programs, The U.S. Department of Agriculture Research, Education, and Economics, and The Department of Homeland Security Science and Technology Directorate*, Washington, DC, June 20, 2019, at https://www.usda.gov/sites/default/files/documents/usda-dhs-moa.pdf. The new facility will be known as the National Bio and Agro-Defense Facility, and is located in Manhattan, KS.

areas of commerce, trade, and public utilities regulation. The distributed enterprise model of critical infrastructure security based on an all-hazards approach potentially elides boundaries between homeland security and other dimensions of infrastructure policy. Likewise, the definition of homeland security itself continues to evolve beyond its counterterrorism roots.

DHS has not submitted a top-level strategy to Congress since the 2014 QHSR. (As noted above, a quadrennial review was due to Congress no later than December 31, 2017.) A more current strategy or other high-level policy statement might serve to more clearly define current Departmental goals, the parameters of its activities related to critical infrastructure security, and how these relate to activities of interagency partners with infrastructure-related responsibilities.

Congressional interest in homeland security strategy was indicated by the Quadrennial Homeland Security Review Technical Corrections Act of 2019 (H.R. 1892), which passed the House of Representatives unanimously and was referred to the Senate Committee on Homeland Security and Governmental Affairs on May 15, 2019. The proposed act would require DHS to consult with relevant advisory committees when developing its capstone strategy, and to more directly link the strategy with budgeting, program management, and prioritization, among other provisions, including new deadlines linked to the budget cycle rather than the end of the calendar year.

Congress has periodically acted to define organizational relationships within DHS. The Department was originally formed with four main directorates, each of which corresponded with a primary homeland security mission. The centralized directorate structure under headquarters management has given way to a more federated structure that emphasizes the operational role and

organizational identity of its operational components.[68] Most recently, the National Protection and Programs Directorate, which administered many of the Department's infrastructure partnership programs, was made an agency within DHS through the 2018 CISA Act. Congress may consider the nature of intra-Departmental organization and relationships within DHS as appropriate, and what degree of centralization or federation best supports the critical infrastructure security mission.

The Role of the Private Sector

Although much of the nation's CI is privately owned, the public may be put at risk if these privately owned critical systems fail. Management of CI risk within a complex ownership and regulatory environment presents enduring policy challenges.

Legislators and other policymakers have generally favored variations of the federated partnership model first elaborated in PDD-63, which relies on voluntary collaboration between the public and private sectors (as opposed to regulatory mandates) to guide investment in critical infrastructure security. Under this model, CI owner-operators, not the government, have ultimate responsibility for assessing and mitigating risk at the enterprise level. At the same time, Congress has directed executive branch agencies to assess and manage risk at the national level. Infrastructure risk management is structured under this framework as a collaborative endeavor between the public and private sectors reliant on incentives, information sharing, and voluntary investments in security.

Public Impacts of Private Business Risk

Businesses protect their productive assets from theft, destruction, and malicious exploitation for business reasons (i.e., to prevent losses and ensure continuity of operations).[69] Private business risks are typically not a matter of public concern as long as consequences of any service disruption are localized and of relatively small scale. However, the modern economy is interconnected and interdependent—so much so that a seemingly minor event may cause cascading failures and lead to a major crisis affecting thousands of businesses and private citizens. This is particularly the case when the business in question is a major utility that provides essential services to the public.

For example, in January 2019, a fire at a small natural gas pumping station in rural Michigan caused an explosion on the coldest day in the year, leading to a much wider crisis. The Michigan governor issued an urgent plea via the Integrated Public Alert Warning System (IPAWS) for residents to turn their thermostats down in order to avoid a catastrophic

[68] DHS operational components include Cybersecurity and Infrastructure Security Agency; U.S. Customs and Border Protection; Federal Emergency Management Agency; Federal Law Enforcement Training Center; U.S. Immigration and Customs Enforcement; U.S. Secret Service; Transportation Security Administration; U.S. Coast Guard; and U.S. Citizenship and Immigration Services.

[69] Many policy documents claim 85% of CI is privately owned. The actual percentage has never been empirically established, and in any case, would vary widely depending on how CI is defined and identified. See Christopher Bellavita, "How Proverbs Damage Homeland Security," *Homeland Security Affairs* vol. 7, no. 2 (2011), p. 2.

Investments in critical infrastructure security in the private sector are largely the purview of private individuals or entities, but many of the most serious risks are borne collectively by the public and larger business community. Under the current partnership structure, government and private-sector representatives collaboratively ascertain what individual enterprise-level investments in security and resilience are necessary to manage CI risk at the societal level.

collapse of the entire gas distribution system. Significant business interests were also affected. Rival gas suppliers curtailed supplies, and automakers were compelled to temporarily shut down production.[70] The Consumers Energy utility incurred costs due to loss of equipment and business interruption, but other businesses also incurred losses, and members of the public were put at risk. The utility's own investigation found that equipment was properly maintained, but that a routine venting process "became hazardous" due to unanticipated effects of high winds.[71]

While there is little question that businesses, government, and society have a "clear and shared interest" in CI resilience, it is often difficult at the policy level to work out exactly who should

[70] John Wisely and Christina Hall, "How Fire and Ice Almost Took Down Michigan's Energy Supply," *The Detroit Free Press*, February 1, 2019, at https://www.freep.com/story/news/local/michigan/2019/02/01/michigan-consumers-energy/2734657002/.

[71] Consumers Energy released results of an internal investigation on April 5, 2019, finding it was not at fault for the incident. The local regulator, the Michigan Public Service Commission, has not yet completed its own analysis as of this writing. https://www.consumersenergy.com/news-releases/news-release-details/2019/04/05/statement-from-consumers-energy-on-the-cause-of-the-january-ray-compressor-fire.

bear responsibility for up-front costs of investment, and what mandatory requirements, regulatory oversight measures, and cost-recovery mechanisms might be necessary in a given case.[72]

Incentives for Private Sector Participation

By and large, the federal government relies upon the private sector to voluntarily develop CI risk management strategies and mitigation investments to support national resilience goals. The 2013 NIPP states that, "Government can succeed in encouraging industry to go beyond what is in their commercial interest and invest in the national interest through active engagement in partnership efforts."[73] In practice, government efforts to encourage voluntary investments in infrastructure resilience through public-private partnerships have varied in extent and effectiveness, particularly when risks in question are diffuse and involve low-probability/high-consequence events such as major terrorist attacks or earthquakes.[74]

The main incentives for industry participation are threefold: improved access to risk information from government sources on security threats and hazards; the value of analyses of national-level risks that exceed the capabilities of most private companies to provide for themselves; and the opportunity to engage with government to influence CI policy.[76] Congress acted to reduce barriers to information sharing between the public and private sectors through the Critical Infrastructure Information Act of 2002, which is designed to ensure confidentiality of industry information shared with DHS in good faith under the Protected Critical Infrastructure Information (PCII) program.[77] Likewise, a number of public-private coordination councils established under the authority of Presidential directives provide a forum for policy discussions and deliberation.

Public-Private Partnerships in Other Countries

The Organization for Economic Cooperation and Development (OECD) released a report in April 2019 on critical infrastructure security policies among member states (including the United States). It found that most members favored voluntary-cooperation frameworks over resilience mandates. However, the report noted that members' CI policy frameworks were relatively immature, and that all faced significant challenges. CI owner-operators might be reluctant to share information "if they fear it will lead to extra costs that they will have to finance, once their vulnerabilities are known," the report stated, adding that such programs can inadvertently create incentives for free-riding by companies that want the benefits of increased overall system resilience without contributing to it themselves by risking proprietary information.[75]

A 2019 report by the Organization for Economic Cooperation and Development (OECD) found that voluntary information sharing and collaboration partnerships in advanced industrialized

[72] Quoted text, see U.S. Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, Executive Summary, 2013*, p. 1.

[73] Ibid., p. 2.

[74] See Hayes, James K., and Charles K. Ebinger, "The Private Sector and the Role of Risk and Responsibility in Securing the Nation's Infrastructure," *Journal of Homeland Security and Emergency Management*, vol. 8, no. 1, 2011; May, Peter J., and Chris Koski, "Addressing Public Risks: Extreme Events and Critical Infrastructures," *Review of Policy Research*, vol. 30, no. 2, 2013, pp. 139-159. Hayes et al.'s statistical study suggests social altruism plays a role in private-sector investment decisions, but that financial cost-benefit calculations predominate among respondents in a survey. May et al. highlight cognitive, behavioral, and organizational barriers to collaboration and investment.

[75] OECD, op. cit., p. 52.

[76] U.S. Department of Homeland Security, NIPP 2013, op. cit., pp. 1-2.

[77] P.L. 107-296 §2222. The PCII program contains protections against disclosure of sensitive CI information for lawsuits, regulatory action, or Freedom of Information Act requests, and establishes standards for government agencies' handling of sensitive information provided by private sector entities.

economies "[do not] necessarily guarantee a strong enough incentive structure to ensure that sufficient investments are effectively made to attain expected resilience targets."[78] Most developed countries augment voluntary policy instruments with regulatory mandates to spur investments in resilience in certain sectors.[79] Regulatory mandates tend to be favored for CI sectors or sub-sectors where incident impacts are potentially catastrophic and elicit broad public concern, such as nuclear meltdowns, gas pipeline explosions, airliner crashes, or terrorist theft of chemicals for use in explosives.[80] According to an academic survey of public-private partnerships for CI security, collaborative approaches more broadly apply "as risks become more privatized" and "harms are more divisible and isolated with respect to their impacts."[81]

Federal Regulation

Policymakers have generally sought to limit the regulatory reach of government within CI security enterprise. For example, PDD-63 stated that "we should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector."[82] The Homeland Security Act created an organization—DHS—with wide-ranging responsibilities, but relatively narrow regulatory mandates. The Transportation Security Administration has (but does not exercise) regulatory oversight over oil and gas pipeline security.[83] The Coast Guard regulates certain aspects of port security—a mission that long predates the transfer of the service to DHS under the Homeland Security Act. Finally, CISA directly regulates certain chemical facilities under the Chemical Facilities Anti-Terrorism Standards program to prevent terrorist exploitation of the chemical industry.

Many other federal, state, and local agencies exercise regulatory authorities that are related to infrastructure security, but are not necessarily specific to homeland security. For instance, the Nuclear Regulatory Commission (NRC) regulates civilian nuclear facilities and enforces extensive safety and reporting requirements. Many of these requirements are traceable to the partial reactor meltdown at Three Mile Island in 1979, and as such are treated as industrial safety and reliability issues in most cases.[84] Many of the aspects of infrastructure security most relevant to homeland security, such as facility protection against deliberate attacks, are overseen by the NRC, not DHS.[85]

---

[78] Organization for Economic Cooperation and Development, *Good Governance for Critical Infrastructure Resilience*, OECD Reviews of Risk Management Policies, Paris, 2019, p. 56.

[79] Ibid., p. 84.

[80] See P. W. Huber, "The Bhopalization of U.S. Tort Law," *Issues in Science and Technology*, 2/1, 1985, pp. 73–82; David Demeritt, Henry Rothstein, Anne-Laure Beaussier, and Michael Howard, "Mobilizing Risk: Explaining Policy Transfer in Food and Occupational Safety Regulation in the UK," *Environment and Planning*, A 47, no. 2, 2015, pp. 373-391.

[81] May et al., op. cit., p. 156.

[82] Presidential Decision Directive 63, p. 3.

[83] CRS Report R44939, *Cybersecurity for Energy Delivery Systems: DOE Programs*, by Paul W. Parfomak, Chris Jaikaran, and Richard J. Campbell. The authors find that TSA relies upon, "voluntary industry compliance with the agency's security guidance and best practice recommendations," despite regulatory and inspection authorities granted to the Agency under the 9/11 Commission Act.

[84] U.S. Nuclear Regulatory Commission, "Backgrounder on the Three Mile Island Accident," at https://www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html.

[85] U.S. Department of Homeland Security, Nuclear Reactors, Materials, and Waste Sector-Specific Plan: An Annex to the NIPP 2013, 2015, p. 2. See CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John D. Moteff, for more examples of non-DHS federal regulation of critical infrastructure security. DHS maintains a support component to coordinate multi-jurisdictional efforts to detect or interdict radiological materials "that are out of regulatory control" named the Countering Weapons of Mass Destruction Office.

Agencies with dual responsibilities for regulation and partnership typically separate the two roles—a lesson learned from early experience with NIPC, which was not clearly separated from the law-enforcement functions of the FBI, and thus had difficulty eliciting participation from private sector entities in its early stages. (See "From the 1990s to the Homeland Security Act" section). The preponderance of DHS infrastructure security programs focus on enhancing voluntary collaboration with infrastructure security partners through development of information sharing, analysis, training, and coordination capabilities, as well as voluntary on-site assessments in certain cases.

The Voluntary CI Partnership Structure

Current CI partnership structures are organized under the authority of PPD-21. The directive is implemented through sector and cross-sector partnership structures described in the 2013 NIPP. The 2013 NIPP outlined an infrastructure protection effort that was less centralized and less focused on critical asset protection than previous iterations of the NIPP, instead emphasizing distributed responsibility among an expansive group of stakeholders committed to common national resilience goals. NIPP partnerships at the federal level are administered by CISA in partnership with other DHS components, and other federal departments and agencies.

Government Coordinating Councils and Sector-Specific Agencies

Each of the 16 CI sectors under the NIPP framework has its own Government Coordinating Council (GCC) and Sector Coordinating Council (SCC). GCCs are made up of federal and SLTT agencies, and, according to the NIPP, enable "interagency, intergovernmental, and cross-jurisdictional coordination" on infrastructure issues of common concern.[86] Each GCC is led by a designated federal agency with sector-relevant responsibilities and expertise, known as a Sector-Specific Agency (SSA). DHS leads or co-leads 10 of the 16 GCCs as the SSA. Other SSAs include the Environmental Protection Agency, the Government Services Agency, and the departments of Agriculture, Defense, Energy, Health and Human Services, Transportation, and Treasury. (See **Table 1** for description of CI sectors and SSAs, and **Appendix C** for visualization of CI partnership structure).

SSAs leverage various NIPP partnership structures to formulate sector-specific infrastructure protection plans that support the overall goals of the NIPP, taking unique sector characteristics and requirements into account. The sector-specific plans contain broad analyses of sector risks, interdependencies with other CI sectors, and stakeholders and partners, which together are used to develop sector-specific resilience goals and measures of effectiveness.

Sector Coordinating Councils

Each SCC is made up of private-sector trade associations and individual CI owner-operators.[87] SCCs are self-organized and self-governed, but must be recognized by the corresponding GCC as

[86] NIPP 2013, Partnership Structure, op. cit., p. 12.

[87] According to the 2018 Critical Infrastructure Partnership Advisory Council (CIPAC) Charter, "Critical infrastructure owners and operators are those entities that own and invest in physical and cyber infrastructure assets, in the systems and processes to secure them, and that are held responsible by the public for their operations and response and recovery when their infrastructure or key resources are disrupted." See U.S. Department of Homeland Security, "Charter of the Critical Infrastructure Partnership Advisory Council," November 30, 2018, at https://www.dhs.gov/publication/cipac-charter.

"appropriately representative" of the sector.[88] They have an advisory relationship with the federal government, and also have coordination and information-sharing functions between government and private-sector stakeholders. SCCs may also support independently organized Information Sharing and Analysis Centers (ISACs) specific to their sector to facilitate information sharing among stakeholders. The National Council of ISACs currently lists 24 member organizations.[89] ISACs maintain operations centers, deploy representatives to the National Cybersecurity and Communications Integration Center (NCCIC) and National Infrastructure Coordinating Center (NICC), conduct preparedness exercises, and prepare a range of informational products for their members. Reliable data on the scale and scope of private-sector participation in SCC activities across CI sectors is not available, but it varies widely depending on sector characteristics.

Cross-Sector Councils

Four cross-sector councils serve to represent key stakeholder groups whose broad interests are not specific to one sector. The State, Local, Territorial, and Tribal Government Coordinating Council (SLTTGCC) is intended to enhance infrastructure resilience partnerships between SLTT jurisdictions, and to represent their common governance-related interests in GCC and SCC deliberations.[90] The Critical Infrastructure Cross-Sector Council consists of the chairs and vice-chairs of the SCCs, and coordinates cross-sector issues among private-sector CI stakeholders. The Regional Consortium Coordinating Council represents regional CI resilience coalitions and encourages sharing of best practices among them.[91]

The Federal Senior Leadership Council (FSLC) is composed of senior officials from federal departments and agencies responsible for implementation of the NIPP, and is chaired by the CISA Director or his designee. It exercises leadership over the other cross-sector councils. According to its charter, the FSLC forges policy consensus among federal agencies on CI risk management strategies, coordinates "issue management resolution" among the other cross-sector councils, develops coordinated resource requests, and advances collaboration with international partners, among other activities.[92]

Advisory Councils

The various NIPP partnership councils may organize certain deliberations under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC), which was first established in 2006. The CIPAC Charter has been renewed several times since then, most recently in 2018. Under certain circumstances, CIPAC provides NIPP coordinating councils and member organizations legal exemption from Federal Advisory Committee Act (FACA) provisions for open meetings, chartering, public involvement, and reporting in order to facilitate discussion between CI stakeholders on sensitive topics relating to infrastructure security.[93] CIPAC engages its

[88] Ibid., p.3.

[89] National Council of ISACs, at https://www.nationalisacs.org/.

[90] According to CIPAC 2018 CI Summit Summary, "SLTTGCC membership spans the ten [FEMA] regions, and is organized into six working groups examining a broad range of critical infrastructure issues such as unmanned aircraft systems, elections infrastructure, cybersecurity, information sharing, and national policy." See Critical Infrastructure Partnership Advisory Council, *2018 Critical Infrastructure Summit*, Summary, p. 3.

[91] Regional Consortium Coordinating Council, *Charter*, March 6, 2018, at https://www.dhs.gov/publication/rc3-charter.

[92] The Federal Senior Leadership Council, *Charter*, March 15, 2019, at https://www.dhs.gov/publication/fslc-charter.

[93] Exemptions from FACA are made by the DHS Secretary under authority of section 87l(a) of the Homeland Security Act, 6 U.S.C. §451(a). For more information on FACA regulations, see CRS Report R44253, *Federal Advisory Committees: An Introduction and Overview*, by Meghan M. Stuessy.

government and private-sector stakeholders through the NIPP partnership structure to develop consensus policy advice and recommendations for DHS and other relevant agencies.

The Homeland Security Advisory Committee (HSAC) provides advice and recommendations to the Secretary of Homeland Security on matters related to homeland security. Members are appointed by the Secretary, and include leaders from state and local government, first responder communities, the private sector, and academia. The Secretary may also establish subcommittees to focus attention on specific homeland security issues as needed. CI-relevant subcommittees have focused on cybersecurity and emerging technologies.

The National Infrastructure Advisory Council is a committee made up of senior industry leaders who advise the President and SSAs on CI policy. It is not formally part of the NIPP partnership structure, but plays an intermediary role between the various coordination councils, the Secretary of Homeland Security, and the President by providing a mechanism for consultation between public and private sector representatives at the highest levels of government. First established by executive order on October 16, 2001, it is tasked with monitoring "the development and operations of critical infrastructure sector coordinating councils and their information sharing mechanisms" and encouraging private industry to improve risk management practices, among other activities.[94]

This partnership structure is more flat than hierarchical, and is realized in multiple formats to include symposia, research collaborations, working groups, policy deliberations, and emergency preparedness and response activities. By design, participation in these activities often crosses organizational lines and includes governmental and non-governmental stakeholders. Increasingly, partnership activities include representatives from multiple CI sectors, due to recognition of the interdependencies inherent in complex CI systems and the general policy trend favoring system resilience over asset protection.[95]

Operational Elements of the Partnership System

The distributed partnership structure has several operational elements maintained by DHS that provide centralized hubs for various non-regulatory coordination and information sharing functions. The National Infrastructure Coordinating Center (NICC) collects, analyzes, and shares threat or other operational information throughout the critical infrastructure partnership network on a real-time basis. It also conducts training and exercises and provides decision support to private sector partners. It is part of the DHS National Operations Center, which serves as the principal operations center for the Department of Homeland Security. Additionally, the National Cybersecurity and Communications Integration Center (NCCIC) serves as a monitoring and incident response center for incidents affecting cybersecurity and communications networks, and also performs several related analytic functions. CISA administers both the NICC and the NCCIC.

Assessing the Effectiveness of This Approach

The underlying policy premise of the current partnership system is that removing or mitigating disincentives to information sharing and increasing trust between the public and private sector

[94] Executive Order 13231, "Critical Infrastructure Protection in the Information Age," p. 3; and U.S. Department of Homeland Security, National Protection and Programs Directorate, *National Infrastructure Advisory Council Charter*, December 11, 2017, pp. 1-2, at https://www.dhs.gov/publication/niac-charter.

[95] OECD, op. cit., p. 3.

will lead to greater industry willingness to invest in system-level resilience. Three related questions may be considered:

- To what extent are private sector owner-operators actually embracing collaboration and information-sharing initiatives offered by federal departments and agencies under the current partnership system?
- Is private-sector participation in these initiatives incentivizing effective investments (beyond those made for business reasons) in programs to reduce overall *public* risk?
- What legislative remedies are appropriate in cases where broader and more effective investments in risk reduction are necessary?

Given the diversity and breadth of the critical infrastructure enterprise as currently defined, the answers to these questions vary across sectors. Rigorous empirical analyses that might shed light on the extent and effectiveness of collaboration within the voluntary framework are scarce.

A 2013 study found that fewer than half of the 16 CI sectors had strong "communities of interest" that actively engaged in CIP issues through NIPP partnership structures. CI communities of interest were strongest in those sectors with strong trade or professional associations unified by relatively specific threats posing individual risk to member companies.[96] A 2011 study found that the most important factor in private-sector risk mitigation investment is a company's own cost-benefit analysis; and that many CI owner-operators believed government will (or should) cover externalized social costs incurred by loss or disruption of company facilities due to a terrorist attack.[97]

GAO testimony provided to Congress in 2014 asserted that DHS partnership efforts faced challenges, and identified three key factors that impact effectiveness of the partnership approach:

- recognizing and addressing barriers to sharing information,
- sharing the results of DHS assessments with industry and other stakeholders, and
- measuring and evaluating the performance of DHS's partnership efforts.

GAO found that DHS did not systematically collect data on reasons for industry participation or non-participation in security surveys and vulnerability surveys, and whether or not security improvements were made as a result.[98] GAO asserted that DHS cannot adequately evaluate program effectiveness absent these measures.

Although DHS concurred and agreed to corrective measures, GAO reported that it had not verified DHS's progress in implementing them.[99] Overall, the picture that emerges from this testimony and other sources is one of extensive partnership activity across multiple CI sectors, but relatively few measures to systematically assess effectiveness of this activity in meeting CI resilience goals.[100]

---

[96] May et al., op. cit., pp. 151-153.

[97] Hayes et al., ibid.

[98] U.S. Government Accountability Office, *Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Approach*, GAO-14-464T, March 26, 2014, p. 15.

[99] Ibid., p. 17.

[100] In 2018, DHS indicated it would survey industry partners in the electricity sub-sector to ascertain what correlations—if any—existed between industry awareness of risks posed by electromagnetic hazards, exposure to DHS information sharing initiatives, and investment in mitigation measures. U.S. Department of Homeland Security,

Issues for Congress

Congress may explore the progress DHS has made in implementing GAO recommended data gathering and analysis initiatives. Availability of data and rigorous analyses may enable Congress to better ascertain the effectiveness of the partnership system in incentivizing industry information sharing and investments in risk reduction.

CISA and its predecessor organizations have not been able to provide reliable data indicating the reach and effectiveness of public-partnership programs in incentivizing bidirectional information sharing and efficient private investments in national level (as opposed to enterprise level) resilience. (The volume and quality of industry information shared with DHS through the PCII program may be one of several useful indicators of program effectiveness.) Congress may address this gap, such as through introduction of appropriate reporting requirements.

Congress may also consider enhancement of regulatory authorities of federal departments and agencies as appropriate to meet national CI resilience goals in cases where voluntary measures do not result in effective industry action to mitigate risk, or emergent threats make immediate action necessary. One recent example is the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which expands the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS) to prevent foreign adversaries from exploiting the legitimate trade system to gain control of CI assets or related information.[101]

Likewise, Congress may exercise oversight in cases where regulatory authorities related to infrastructure security exist but are not exercised, as in the case of TSA described above.

CISA plans to maintain the current sector specific public-private partnership structures as the preferred vehicle for information sharing and policy coordination. Congress may consider whether adjustment or replacement of these structures is needed to streamline and better align partnership efforts with the emerging federal risk management approach, which emphasizes inter-sectoral analysis and resilience rather than sector-specific asset identification and protection.

Strategy for Protecting and Preparing the Homeland Against Threats of Electromagnetic Pulse and Geomagnetic Disturbances, October 9, 2018, p. 12. This appears to be an isolated initiative that has yet to be implemented.

[101] P.L. 115-232, Foreign Investment Risk Review Modernization Act of 2018, Sec. 1701(c). For more information on CFIUS, see CRS Report RL33388, *The Committee on Foreign Investment in the United States (CFIUS)*, by James K. Jackson.

Appendix A. National Critical Functions

"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."

Connect	Distribute	Manage	Supply
Operate Core Network	Distribute Electricity	Conduct Elections	Exploration and Extraction of Fuels
Provide Cable Access Network Services	Maintain Supply Chains	Develop and Maintain Public Works and Services	Fuel Refining and Processing Fuels
Provide Internet Based Content, Information, and Communication Services	Transmit Electricity	Educate and Train	Generate Electricity
Provide Positioning, Navigation, and Timing Services	Transport Cargo and Passengers by Air	Enforce Law	Manufacture Equipment
Provide Radio Broadcast Access Network Services	Transport Cargo and Passengers by Road	Maintain Access to Medical Records	Produce and Provide Agricultural Products and Services
Provide Satellite Access Network Services	Transport Cargo and Passengers by Vessel	Manage Hazardous Materials	Produce and Provide Human and Animal Food Products and Services
Provide Wireless Access Network Services	Transport Materials by Pipeline	Manage Wastewater	Produce Chemicals
Provide Wireline Access Network Services	Transport Passengers by Mass Transit	Operate Government	Provide Metals and Materials
		Perform Cyber Incident Management Capabilities	Provide Housing
		Prepare for and Manage Emergencies	Provide Information Technology Products and Services
		Preserve Constitutional Rights	Provide Materiel and Operational Support to Defense
		Protect Sensitive Information	Research and Development
		Provide and Maintain Infrastructure	Supply Water
		Provide Capital Markets and Investment Activities	
		Provide Consumer and Commercial Banking Services	
		Provide Funding and Liquidity Services	

Connect	Distribute	Manage	Supply
		Provide Identity Management and Associated Trust Support Services	
		Provides Insurance Services	
		Provide Medical Care	
		Provide Payment, Clearing, and Settlement Services	
		Provide Public Safety	
		Provide Wholesale Funding	
		Store Fuel and Maintain Reserves	
		Support Community Health	

Source: CISA, "National Critical Functions Set," at https://www.dhs.gov/cisa/national-critical-functions-set.

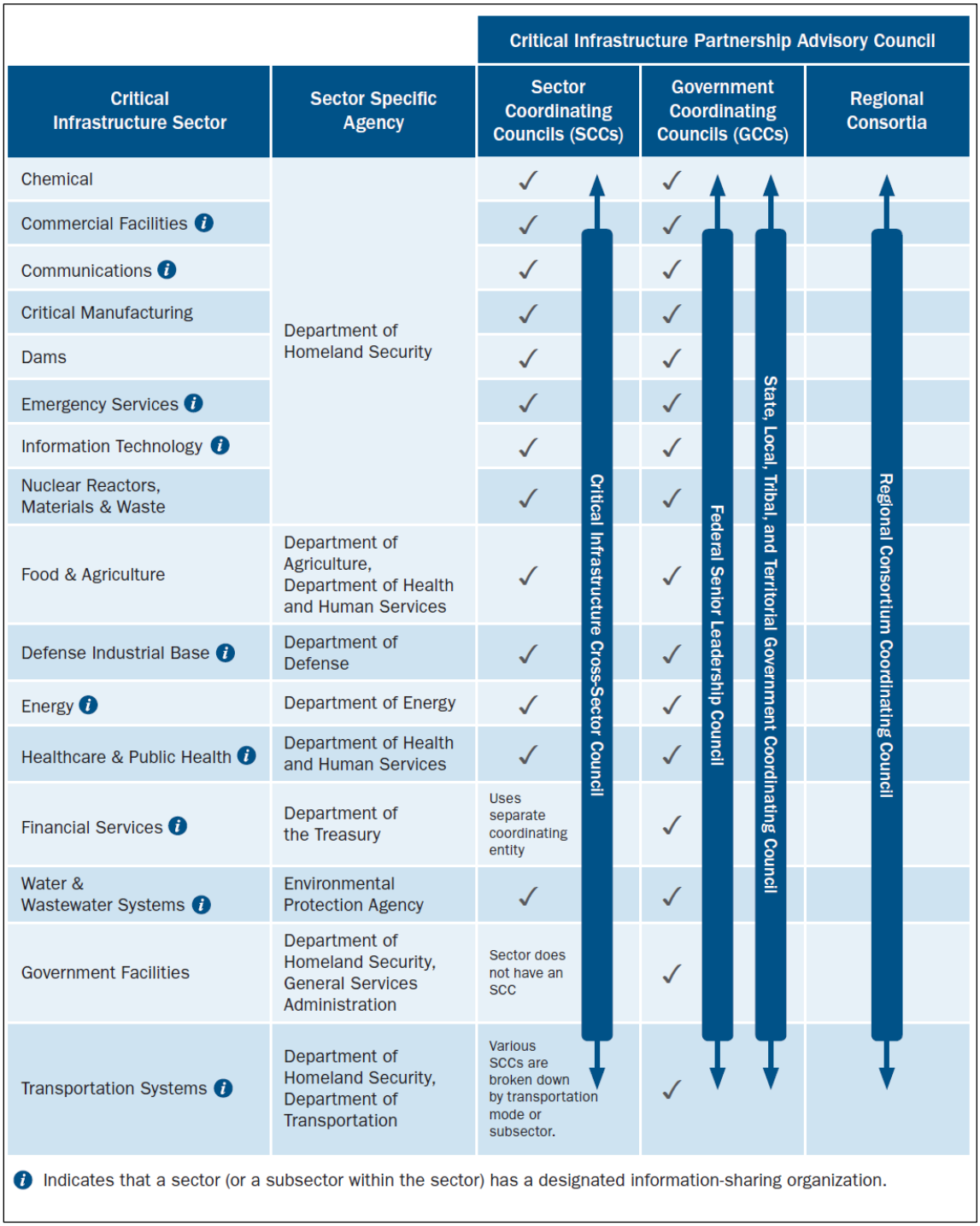
Appendix B. Key Terms

Glossary

Critical Infrastructure (CI)	Machinery, facilities, and information that enable vital functions of governance, public health, and the economy.
Critical Infrastructure Protection (CIP)	Policy approach that emphasizes the identification, prioritization, and protection of infrastructure assets. Criticality from this perspective is generally defined in terms of consequences (i.e., an infrastructure asset or system is critical to the degree that loss or disruption of service would have system-level impacts on essential functions of society, the economy, or government).
Critical Infrastructure Resilience (CIR)	Policy approach that defines criticality in terms of capabilities necessary to maintain essential functions, emphasizing broad investments in hazard mitigation and preparedness during steady-state periods and adaptation during emergencies to ensure continued provision of essential services.
Critical infrastructure system	Interconnected physical or cyber assets that enable provision of critical services.
Cybersecurity and Infrastructure Security Agency (CISA)	Operational component of DHS directly responsible for national CI risk management and administration of public-private partnership system established by PPD-21 and NIPP 2013. CISA also administers Chemical Facility Anti-Terrorism Standards program and DHS CI information hubs (NICC and NCCIC).
Gilmore Commission	A congressional blue-ribbon panel chartered in 1999 to study the threat of terrorist use of weapons of mass destruction.
Government Coordinating Council (GCC)	GCCs are made up of federal and SLTT agencies, and, according to the NIPP, enable "interagency, intergovernmental, and cross-jurisdictional coordination" on infrastructure issues of common concern.
Hart-Rudman Commission	Blue ribbon panel chartered by DOD in 1998 to study 21st century security issues. The panel favored creation of a new federal homeland security agency. Many recommendations were incorporated into the Homeland Security Act of 2002.
Homeland Infrastructure Foundation—Level Data (HIFLD)	National foundation-level geospatial data within the public domain provided by the federal government to support community preparedness, resiliency, research, and other CIR activities.
Homeland Security Act of 2002	Created the Department of Homeland Security. Subsequent CI related bills have frequently been formulated as amendments to the act (P.L. 107-296).
Homeland Security Advisory Council (HSAC)	Provides advice and recommendations to the Secretary of Homeland Security on matters related to homeland security. Membership includes leaders from state and local government, first responder communities, the private sector, and academia.
Homeland Security Presidential Directive 7 (HSPD-7)	Post-9/11 directive released in 2003 that first formalized CI sectors and coordinating councils, focusing on asset identification and protection.
National Asset Database	Congressionally mandated compilation of vital systems or assets that the Secretary of Homeland Security determines may cause national or regional catastrophic effects if subject to disruption or destruction.
National Critical Infrastructure Prioritization Program (NCIPP)	An identification and prioritization program instituted by DHS to fulfil the Congressional mandate for the National Asset Database. The NCIPP list is a classified compendium of assets identified and nominated by SLTT and other stakeholders, and vetted by DHS according to consequence-based criteria of fatalities, economic loss, mass evacuation length, and national security impacts.

National Cybersecurity and Communications Integration Center (NCCIC)	Serves as a monitoring and incident response center under CISA auspices for incidents affecting cybersecurity and communications networks, and also performs several related analytic functions.
National Infrastructure Protection Plan (NIPP)	National-level plans developed under the Bush and Obama administrations to establish strategic goals for infrastructure security, and to define interagency relationships and public-private partnerships.
National Risk Management Center (NRMC)	CISA has established the National Risk Management Center (NRMC) as a "planning, analysis, and collaboration center" to manage national CI risk in partnership with federal, SLTT, and private-sector stakeholders.
Operational Components of DHS	Component agencies of DHS with operational mission responsibilities. These include: Cybersecurity and Infrastructure Security Agency; U.S. Customs and Border Protection; Federal Emergency Management Agency; Federal Law Enforcement Training Center; U.S. Immigration and Customs Enforcement; U.S. Secret Service; Transportation Security Administration; U.S. Coast Guard; and U.S. Citizenship and Immigration Services.
Presidential Decision Directive 63 (PDD-63)	Clinton-era directive signed in 1998 commonly cited as first high-level policy guidance for critical infrastructure protection in the contemporary era.
Presidential Policy Directive 21 (PPD-21)	Policy guidance released by Obama White House in 2013 for critical infrastructure security, superseding HSPD-7. Maintains much of the previous policy framework of HSPD-7, but places greater emphasis on all-hazards resilience and highly distributed public-private partnerships. Remains in force as of this writing.
Protected Critical Infrastructure Information (PCII)	DHS program established under provisions of the Critical Infrastructure Information Act of 2002, which ensures confidentiality of certain industry CI information shared with the government in good faith. It contains protections against disclosure for lawsuits, regulatory action, or Freedom of Information Act requests.
Sector Coordinating Council (SCC)	Self-organized and self-governed councils composed of critical infrastructure owners and operators, their trade associations, and other industry representatives. SCCs coordinate and collaborate with SSAs and related GCCs on the entire range of critical infrastructure security and resilience policies and efforts for a given CI sector.
Sector-Specific Agency (SSA)	Federal government agency with knowledge and responsibilities specific to a given CI sector assigned primary responsibility for implementation of PPD-21 in that sector.
The National Infrastructure Coordinating Center (NICC)	NICC collects, analyzes, and shares threat or other operational information throughout the critical infrastructure partnership network on a real-time basis. It also conducts training and exercises and provides decision support to private sector partners. It is part of the DHS National Operations Center, which serves as the principal operations center for DHS.
USA PATRIOT Act of 2001	The USA PATRIOT Act (P.L. 107-56) contains numerous homeland security related provisions that expand law enforcement authorities. It defines critical infrastructure as "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." This definition has been widely adopted in other laws and policy documents.

Appendix C. Sector and Cross-Sector Coordinating Structures



Source: NIPP 2013, "Sector and Cross-Sector Coordinating Structures," at https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.

Author Information

Brian E. Humphreys
Analyst in Science and Technology Policy

Disclaimer