Congressional Research Service
Informing the legislative debate since 1914

Critical Infrastructure: Emerging Trends and Policy Considerations for Congress

March 10, 2026

Congressional Research Service
https://crsreports.congress.gov
R48878

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R48878

March 10, 2026

Brian E. Humphreys
Analyst in Science and Technology Policy

Critical Infrastructure: Emerging Trends and Policy Considerations for Congress

Critical infrastructure refers to the machinery, facilities, and information systems that enable critical functions of governance, public health, and the economy. Risks to infrastructure include terrorism, organized crime, cyberattacks, and hostile action by foreign governments, as well as natural hazards, accidents, and aging or obsolescence of infrastructure. Much of this infrastructure is privately owned, but risks to critical assets are often a shared public concern.

In recent decades, critical infrastructure stakeholders in government and the private sector have developed the national critical infrastructure security and resilience (CISR) enterprise to manage risk to critical infrastructure systems and assets and to ensure continuity of critical functions at a broader societal level—both during steady-state situations and during contingencies that stress critical infrastructure systems beyond normal operating limits. Successive Administrations and Congresses have acted to expand federal agencies' roles and responsibilities in the public-private partnerships that define the CISR enterprise. Four areas of enduring concern are defining and identifying critical infrastructure, understanding and assessing critical infrastructure risk, organizing federal resources to address critical infrastructure, and encouraging public-private partnerships.

The Critical Infrastructures Protection Act of 2001 (CIPA; P.L. 107-56, §1016) defined *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 focused on identification and protection of critical systems and assets. Early federally led efforts to comprehensively survey critical systems and assets on the basis of this definition often lacked methodological rigor and provided inconsistent results. Subsequent reforms and legislation directed agencies to make methodological changes and establish the National Asset Database, which is populated primarily via state government nominations.

Perceived limitations of asset-centric approaches to protecting critical infrastructure led to a broader shift within the CISR enterprise toward function-centric approaches that prioritized increasing resilience of complex interdependent systems as a whole. Function-centric approaches seek to make any single component or asset of these systems less critical. Such approaches have emphasized assessment of interdependencies between major infrastructure systems, development of consensus resilience standards within relevant industries, creation of contingency plans and training, and incorporation of redundancies into system design. In practice, federal CISR policies, programs, and activities combine elements of both asset-centric and function-centric approaches to risk management.

The Cybersecurity and Infrastructure Security Agency (CISA), established by Congress in 2018 as part of the Department of Homeland Security (DHS), is the designated National Coordinator for CISR programs and activities. It oversees public-private partnerships across 16 designated critical infrastructure sectors in coordination with other federal agencies. These partnerships have been structured by coordinating bodies that have facilitated confidential discussions and information sharing on critical infrastructure issues between public and private-sector stakeholders. They also include operational components such as Information Sharing and Analysis Centers that collect and share information on risk and no-cost cybersecurity and physical security services provided by CISA. Observers have offered mixed assessments of the effectiveness of these partnerships. In some cases, government partnership initiatives have drawn little interest, while in other cases, they appear to have contributed to the growth of vibrant communities of interest.

In 2025, the Trump Administration eliminated the previous legal framework for confidential public-private coordination on infrastructure issues and submitted budget proposals that would curtail the scale and scope of existing partnerships. However, media reports indicate that a new framework with unspecified reforms is in active consideration as of early 2026. If it chooses to act, Congress may reinforce—and perhaps reform—the previously established system of public-private partnerships. Alternatively, it may legislatively ratify the Administration's proposal to move toward a more localized risk management framework and transfer core CISR governance functions to the states. Should Congress choose the former, it may consider legislation to reestablish a legal framework for public-private partnerships, to include provisions for confidential discussions and sharing of sensitive infrastructure information. Should it choose the latter, it may consider supporting state and local efforts to take increased responsibility for ensuring resilience of critical infrastructure functions in their jurisdictions. If fully enacted, these policies would likely give rise to a diverse set of more localized CISR risk management enterprises in place of the national-scale system.

Contents

Introduction 1
Defining and Identifying Critical Infrastructure 2
Presidential Decision Directive 63 2
Statutory Definition of Critical Infrastructure 3
Risk Management: Asset Protection and Infrastructure Resilience 4
Asset Protection Approaches to Risk Management 5
The 9/11 Commission Act of 2007 and the National Asset Database 6
Other Asset Identification Mandates, Authorities, and Guidelines 7
Resilience-Based Approaches to Risk Management 8
National Critical Functions 9
Cyber Incident Reporting for Critical Infrastructure Act of 2022 and Identification of Critical Infrastructure Entities 10
National Security Memorandum 22 11
Federal Organization for Critical Infrastructure Risk Management 11
From the 1990s to the Homeland Security Act of 2002 12
Consolidation and the Creation of DHS 13
Policy and Budgetary Implications of Organizational Change 13
Evolution of Critical Infrastructure Policy Since the Establishment of DHS 14
Transition to All-Hazards Approach 15
Role and Organization of CISA 16
CISA Regulatory Authorities 16
CISA Services for Critical Infrastructure Sectors 18
Public-Private Partnerships 19
Critical Infrastructure Sectors 20
Public-Private Partnership Coordination Bodies 22
Government Coordinating Councils 23
Sector Coordinating Councils 24
Cross-Sector Councils 25
Other CIPAC Advisory Councils 25
FACA Advisory Councils 25
Incentives for Private-Sector Participation 26
The Relationship Between Voluntary Partnerships and Federal Regulation 28
Assessing the Effectiveness of Voluntary Partnerships 29
Potential Revisions to the All-Hazards Approach and Increased Role of States in Risk Management 32
Stakeholder Perspectives on E.O. 14239 33
Proposed CISA FY2026 Budget 33
Congressional Appropriations for FY2026 35
Other Legislation 35
Policy Options and Considerations for Congress 36
Shift Responsibility to State and Local Governments 36
Considerations for Federal and State Collaboration 36
Other Policy Considerations 37

Figures

Figure C-1. Sector and Cross-Sector Coordinating Structures 44

Tables

Table 1. Critical Infrastructure Sectors 21
Table 2. CISA FY2026 Budget Justification 34

Table A-1. Glossary of Key Terms 39
Table B-1. National Critical Function Set 42

Appendixes

Appendix A. Glossary of Key Terms 39
Appendix B. National Critical Functions 42
Appendix C. Sector and Cross-Sector Coordinating Structures 44

Contacts

Author Information 45

Introduction

Critical infrastructure refers to the machinery, facilities, and information systems that enable critical functions of governance, public health, and the economy. Deficiencies within the networks of expertise, governance, and economic relationships in which critical infrastructure systems and assets are embedded may increase risks posed by natural and human-caused hazards.

In recent decades, critical infrastructure stakeholders in government and the private sector have developed the national critical infrastructure security and resilience (CISR) enterprise to manage risk to critical infrastructure systems and assets and to ensure continuity of critical functions at a broader societal level—both during steady-state situations and during contingencies that stress critical infrastructure systems beyond normal operating limits.

Federal government agencies have sometimes described their partners in the national CISR enterprise as being part of a critical infrastructure community. This community—more concept than organization—is the aggregate of people and organizations engaged in security and resilience activities related to critical infrastructure. It includes thousands of private-sector businesses and enterprises, nonprofits, researchers, analysts, and technologists, as well as interested legislators, government officials, and law enforcement and emergency management personnel.

At the federal level, the critical infrastructure community is organized under the auspices of presidential policy directives. These assign the Department of Homeland Security (DHS), acting through the Cybersecurity and Infrastructure Security Agency (CISA), responsibility for leadership and interagency coordination of voluntary public-private partnerships across 16 designated critical infrastructure sectors and numerous subsectors. CISA delegates this responsibility to other agencies in some cases. The responsible agency in each sector is referred to as the "sector risk management agency" (SRMA).[1]

Because much of the nation's critical infrastructure is owned and operated by the private sector, implementation of federal initiatives to manage risk often depends on the willingness and ability of private-sector entities to engage with CISR-oriented communities of interest, to make relevant resilience investments, and to report cyber incidents and physical security breaches quickly—even those that may pose reputational, legal, or regulatory consequences. Likewise, owner-operators of vulnerable systems may have to absorb significant up-front business costs to increase security. Owner-operators of systems that do not meet the statutory definition of critical infrastructure may still suffer from attacks that present systemic risk, given the interconnectedness of such systems.

Successive Administrations and Congresses have acted to expand federal agencies' roles and responsibilities—both regulatory and nonregulatory—in the public-private partnerships that define the CISR enterprise. On March 13, 2025, DHS issued directives that terminated certain coordination mechanisms that had, since 2006, facilitated conduct of public-private partnerships and directed executive branch entities to devolve the majority of critical infrastructure risk

[1] Section 9002 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY2021 NDAA; P.L. 116-283) assigns "SRMA" the same meaning as "sector-specific agency" given in 6 U.S.C. §651(5). That statute defines *sector-specific agency* as a "Federal department or agency, designated by law or presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department [of Homeland Security]."

management functions to the states.[2] Several days later, President Trump issued Executive Order (E.O.) 14239, "Achieving Efficiency Through State and Local Preparedness," which called for state and local governments to assume more responsibility for resilience and preparedness.[3] These two policy changes suggest a shift toward a less centralized, more localized critical infrastructure enterprise (see "Potential Revisions to the All-Hazards Approach and Increased Role of States in Risk Management" section).

E.O. 14239 tasked the National Security Advisor (in coordination with relevant agencies) with developing specific policy documents to implement the broad principles and priorities that E.O. 14239 sets forth. As of the date of this report, these policy documents are not available.

This report highlights four key areas of enduring policy concern for Congress vis-à-vis the national CISR enterprise as it develops within an increasingly challenging and complex risk environment. A section is devoted below to each key area: defining and identifying critical infrastructure, managing critical infrastructure risk, organizing federal resources to address critical infrastructure, and encouraging public-private partnerships. This report also discusses the prospect of fundamental changes to the national CISR enterprise during the second Trump Administration. Thus, one of its primary purposes is to provide historical context and a baseline against which to assess potential future policy changes.

Defining and Identifying Critical Infrastructure

Definitions of critical infrastructure have affected which assets, facilities, and systems are assessed for risk and protected.

Presidential Decision Directive 63

Presidential Decision Directive 63 (PDD-63), released by President Clinton in 1998, provided early foundational guidance for critical infrastructure protection (CIP). It framed critical infrastructure risk in terms of national vulnerability to potentially devastating asymmetric attacks.[4] The directive presented U.S. economic and military might as "mutually reinforcing and dependent" elements of national power dependent on critical infrastructure to function properly.[5]

[2] See DHS, "Notice of Termination of Discretionary Federal Advisory Committees," 90 *Federal Register* 11995, March 13, 2025. The notice announces termination of the Critical Infrastructure Partnership Advisory Council (CIPAC), among other entities, in accordance with Executive Order (E.O.) 14217 of February 19, 2025, "Commencing the Reduction of the Federal Bureaucracy," 90 *Federal Register* 10577, February 25, 2025, https://www.federalregister.gov/documents/2025/02/25/2025-03133/commencing-the-reduction-of-the-federal-bureaucracy. Multiple critical infrastructure security and resilience (CISR) public-private coordination bodies operated under CIPAC auspices, which provided the legal and institutional framework for confidential deliberations and information sharing.

[3] E.O. 14239 of March 18, 2025, "Achieving Efficiency Through State and Local Preparedness," 90 *Federal Register* 13267, March 21, 2025, https://www.federalregister.gov/documents/2025/03/21/2025-04973/achieving-efficiency-through-state-and-local-preparedness.

[4] Tami Davis Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing, 1914-1945* (Princeton University Press, 2009), https://www.degruyterbrill.com/document/doi/10.1515/9781400824977/html (hereinafter Biddle, *Rhetoric and Reality in Air Warfare*). The term *asymmetric attacks* denotes attacks in which a militarily weaker attacker uses subterfuge or novel methods to achieve success against an opponent with greater material capabilities.

[5] Presidential Decision Directive 63 (PDD-63), "Critical Infrastructure Protection," May 22, 1998, p. 1, https://irp.fas.org/offdocs/pdd/pdd-63.htm.

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."[6]

PDD-63 directed federal agencies to partner with private-sector stakeholders to "take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems."[7] In practice, the sheer scale and complexity of such systems—even under the relatively limited scope of infrastructure covered by the Clinton-era directive—made it necessary to manage, rather than completely eliminate, risk.[8] The complex interdependent systems that constitute critical infrastructure have continued to evolve rapidly since 1998, presenting policymakers and diverse stakeholder communities with a continuing challenge to identify system-critical assets and to prioritize mitigation actions and investments accordingly.

Statutory Definition of Critical Infrastructure

The definition of critical infrastructure has evolved over time since the concept first emerged in the era between the two world wars (see **text box** below on "Where Did the Concept of Critical Infrastructure Come From?"). The most commonly cited statutory definition of critical infrastructure originated shortly after the 9/11 terrorist attacks in 2001. It was established in the Critical Infrastructures Protection Act of 2001 (CIPA), enacted as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT; P.L. 107-56, §1016). It echoed PDD-63 in its focus on protecting the industrial and demographic foundations of military power against asymmetric threats. The statute defined *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."[9] (For definitions of other key terms, see **Appendix A**.)

The CIPA definition of critical infrastructure remains law and is still commonly cited as a basis for executive branch policy directives and guidance. The statute is frequently incorporated by reference in relevant legislation.[10] The wide use of this definition (and numerous variations based on it) has several implications for federal policy formulation and implementation. Its ubiquity in the federal policy space makes it a common reference point for the multiple agencies and other entities with CISR responsibilities. Likewise, the wide use of this definition and its various derivatives over more than two decades provide a degree of predictability and stability to private-sector stakeholders who participate in voluntary or regulatory critical infrastructure programs.

The statutory definition presupposes certain specific approaches to CISR policy that reflect the counterterrorism-focused security concerns of the 9/11 era. Conceptually, the statutory language is asset-centric and consequence oriented—that is, it privileges "systems and assets" as a category of concern and defines criticality in terms of predicted consequences of asset "incapacity or destruction." Therefore, policy guidance based on this definition frequently emphasizes identification of systems and assets for protection based on assessment of potential adverse

[6] PDD-63.

[7] PDD-63.

[8] PDD-63 named telecommunications, energy, banking and finance, transportation, water systems and emergency services, among other sectors, as critical.

[9] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), §1016(e).

[10] 42 U.S.C. §4195c.

consequences in case of disruption or destruction as the predominant activity of the critical infrastructure risk management enterprise.[11]

Where Did the Concept of Critical Infrastructure Come From?

Awareness of the potential vulnerability of modern infrastructure to deliberate attack or natural disaster dates at least to the era between the two world wars, 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.[12] 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.[13] 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 that threaten infrastructure at the systemic level. (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.)

Risk Management: Asset Protection and Infrastructure Resilience

Critical infrastructure policy has taken on two distinct orientations that significantly overlap but nonetheless reflect different conceptual perspectives and policy priorities—CIP and critical infrastructure resilience (CIR). The national infrastructure risk management enterprise reflects a hybrid approach that contains elements of both CIP and CIR.

CIP emphasizes the identification, prioritization, and protection or hardening of infrastructure *assets*.[14] Criticality from this perspective is generally defined in terms of the consequences of asset loss (i.e., an infrastructure asset is critical to the degree that the loss or disruption of this asset would have systemic-level impacts on essential functions of society, the economy, or government). Risk management activities include identifying the *most* critical systems and assets for hardening and other risk mitigation measures. Much of the major legislation that serves as the foundation for CIP-focused initiatives was passed in the immediate aftermath of the 9/11 attacks, when concerns with physical protection of critical assets against asymmetric attacks predominated in policy circles.[15]

[11] Some non-U.S. definitions include processes, services, organizations, and supply chains, which suggests greater emphasis on societal functions than the U.S. definition. For definitions of critical infrastructure adopted by the "Critical Five" countries (United States, United Kingdom, Australia, New Zealand, and Canada), see Public Safety Canada, *Critical 5: Adapting to Evolving Threats—A Summary of Critical 5 Approaches to Critical Infrastructure Security and Resilience*, Ottawa, Canada, 2024, pp. 20-30.

[12] Biddle, *Rhetoric and Reality in Air Warfare*.

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

[14] *Hardening* in this context refers to augmentation of critical infrastructure assets with physical, virtual, or administrative countermeasures to protect against potential natural or human-caused threats and hazards. For example, shielding of exposed conductors at an electric substation may offer physical protection against the effects of an electromagnetic pulse.

[15] The USA PATRIOT ACT (P.L. 107-56), passed in 2001, provided a statutory definition of critical infrastructure, which is still in wide use. The Homeland Security Act of 2002 (P.L. 107-296) created the Department of Homeland Security (DHS), which administers many critical infrastructure protection (CIP) policies, programs, and activities.

By contrast, CIR emphasizes continuity of critical infrastructure *functions*. From this perspective, critical infrastructure is viewed as a diverse set of complex interconnected and interdependent systems. Critical infrastructure is resilient to the extent that it provides essential functions (electricity, network connectivity, wastewater management, etc.) when some assets are stressed beyond normal design parameters. Risk management activities tend to be broad in scope. They may include assessment of interdependencies between major infrastructure systems, development of consensus resilience standards within relevant industries, creation of contingency plans and training, and incorporation of redundancies into system design. By increasing resilience of complex interdependent systems as a whole, CIR approaches seek to make any single component or asset of these systems less critical.[16]

Asset Protection Approaches to Risk Management

Since 2001, CIP-focused legislation and government policy directives have frequently contained requirements for the creation of asset lists, catalogs, databases, and reports to identify systems and assets that meet the statutory threshold of criticality and thus require higher than ordinary levels of protection against plausible threats.

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 by the George W. Bush Administration just before DHS 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."[17]

It was followed by the December 2003 release of "Homeland Security Presidential Directive 7" (HSPD-7), which served as the basis of critical infrastructure policy development and implementation for the next decade. 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."[18] DHS claimed in the 2006 National Infrastructure Protection Plan (NIPP)—the first plan of its type—that it had compiled a comprehensive critical infrastructure database to meet the critical infrastructure identification requirement.[19]

However, a 2006 DHS Office of Inspector General (OIG) report found that these early efforts to produce a national database of critical infrastructure assets suffered from conceptual and methodological shortcomings.[20] Data calls to states and territories beginning in 2004 produced thousands of asset nominations. The report stated that DHS's National Asset Database had rapidly

[16] Per 42 U.S.C. §17384a(j). *resilience* refers to "the ability to withstand and reduce the magnitude or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, or rapidly recover from such an event, including from deliberate attacks, accidents, and naturally occurring threats or incidents."

[17] See the "Planning and Resource Allocation" section in White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003, p. 23, https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf.

[18] White House, "Homeland Security Presidential Directive 7," December 17, 2003, https://www.dhs.gov/homeland-security-presidential-directive-7.

[19] DHS, *National Infrastructure Protection Plan*, 2006, p. 31, https://www.dhs.gov/xlibrary/assets/NIPP_Plan_noApps.pdf.

[20] DHS, Office of Inspector General, *Progress in Developing the National Asset Database*, OIG-06-40, June 2006, https://www.oig.dhs.gov/sites/default/files/assets/Mgmt/OIG_06-40_Jun06.pdf (hereinafter DHS OIG, *Progress in Developing the National Asset Database*).

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 OIG 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.[21] Likewise, data collection procedures were not standardized, so that, for example, San Francisco listed its entire light rail system as a single asset, while New York City listed its subway stations as multiple individual assets.

The 9/11 Commission Act of 2007 and the National Asset Database

Congress subsequently included provisions for the National Asset Database as part of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Commission Act; P.L. 110-53).

The legislation—based in part on HSPD-7 CIP provisions—required 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 was to include assets that the Secretary of Homeland Security determined would cause national or regional catastrophic effects if they were disrupted or destroyed.[22] Other provisions included definitions of infrastructure-related terms and a requirement for the Secretary to implement certain quality control procedures to ensure that asset nominations from state governments or other sources met the threshold of criticality as determined by the Secretary.[23]

A 2013 Government Accountability Office (GAO) report found that DHS had improved its processes for critical asset identification since passage of the 9/11 Commission Act but that significant questions regarding reporting criteria and methodology persisted.[24] The report documented frequent changes in nomination and adjudication criteria and reporting format used by the 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 asset nominations according to four types of potential adverse consequences above certain designated thresholds: fatalities, economic loss, mass evacuation length, and national security impacts.[25] DHS has made periodic updates to methodology and nomination criteria since then.

According to a March 2022 GAO report, there were 1,404 assets on the list as of May 2021.[26] Of these, 88 were categorized as especially critical Level 1 assets.[27] The remainder were categorized as less-critical Level 2 assets. Some state governments have declined to participate in DHS data calls because of compliance costs and technical limitations.[28] In several cases, states said they

[21] DHS OIG, *Progress in Developing the National Asset Database*, p. 9.

[22] See 6 U.S.C. §664(a)2.

[23] See 6 U.S.C. §664(c)1.

[24] U.S. Government Accountability Office (GAO), *Critical Infrastructure Protection: DHS List of Priority Assets Needs to Be Validated and Reported to Congress*, GAO-13-296, March 2013, https://www.gao.gov/assets/gao-13-296.pdf (hereinafter GAO-13-296).

[25] GAO-13-296, p. 13. Previously, criticality was based on measures of capacity, such as commercial facility occupancy limits and throughput of pipeline.

[26] GAO, *Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing*, GAO-22-104279, March 1, 2022, p. 88, https://www.gao.gov/assets/gao-22-104279.pdf (hereinafter GAO, GAO-22-104279).

[27] GAO-22-104279, p. 88.

[28] GAO-13-296, pp. 30-31.

lacked expertise to develop scenarios and model complex infrastructure systems with sufficient fidelity to assess likely consequences of failure or disruption.[29] The perception that the list was not particularly useful may have also played a role. GAO reports on NCIPP provide a mixed assessment of its usefulness based on interviews with critical infrastructure stakeholders. According to an April 2022 report, "CISA and other critical infrastructure stakeholders GAO spoke with said that the [NCIPP] results were of little use and raised concerns with the program."[30]

Other Asset Identification Mandates, Authorities, and Guidelines

Beyond the identification and designation of critical infrastructure assets for the purpose of infrastructure protection, several statutes grant power to federal authorities to designate systems and assets as critical in certain other contexts. For example, the Cyber Security Enhancement Act of 2002 (P.L. 107-296, §225) directed the U.S. Sentencing Commission to amend sentencing guidelines to provide enhancements for certain violations of the Computer Fraud and Abuse Act (18 U.S.C. §1030) that were "intended to or had the effect of significantly interfering with or disrupting a critical infrastructure." As amended, the sentencing guidelines define *critical infrastructure* as "systems and assets vital to national defense, national security, economic security, public health or safety, or any combination of those matters."[31] This definition is applied by judges in the context of specific sentencing decisions.

Federal law also provides authority (16 U.S.C. §824o-1) to the Secretary of Energy to issue orders to operators of civilian and defense-critical electric infrastructure to implement specified emergency measures during declared grid security emergencies caused by cyber intrusions, electromagnetic pulse attacks, geomagnetic disturbances, or physical attacks. The statute defines *critical electric infrastructure* as a "system or asset of the bulk-power system, whether physical or virtual, the incapacity or destruction of which would negatively affect national security, economic security, public health or safety, or any combination of such matters." The statute allows the Secretary of Energy full discretion to apply this definition as necessary during a declared grid emergency, in consultation with Canadian and Mexican authorities, relevant U.S. critical infrastructure coordinating bodies, and "appropriate" U.S. federal agencies "to the extent practicable."

In March 2020, CISA issued guidelines on critical infrastructure workforces to assist state and local authorities in formulating exemptions to broad workplace closure directives during the COVID-19 pandemic. Some Administration officials and business leaders cited these guidelines as the authoritative basis for workforce management directives that asserted exemptions from state and local workplace closure directives. In some cases, labor groups and local authorities contested these assertions. According to CISA, the guidelines were advisory. However, some states incorporated the CISA guidelines by reference into policies on exemptions from mandatory

[29] GAO-13-296, p. 30, and GAO, *Critical Infrastructure Protection: DHS Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure*, GAO-22-105973, April 6, 2022, https://www.gao.gov/assets/gao-22-105973.pdf (hereinafter GAO-22-105973).

[30] GAO-22-105973. The report also raised concerns with methodology: "Senior officials with CISA, as well as other federal, state, and private sector officials we spoke with said that the consequence thresholds for these criteria did not reflect the current threat environment, which focuses more on cyberattacks and extreme weather events. The threat environment also focuses on vulnerabilities or attacks that can affect multiple entities within a short period. In this scenario, the consequences related to a single asset, entity, system, or cluster may not reach [National Critical Infrastructure Prioritization Program] thresholds, but the aggregate impacts may be nationally significant, according to CISA officials" (p. 11).

[31] U.S. Sentencing Commission, *Guidelines Manual*, 2025, p. 90, https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2025/GLMFull.pdf.

workplace closures, giving the guidelines legal status within their jurisdictions. According to an article in the *National Law Review*, state and local authorities—not federal agencies—assumed responsibility for adjudicating claims of criticality made by private-sector stakeholders in these cases.[32]

Resilience-Based Approaches to Risk Management

CIR approaches prioritize adaptive use of available capabilities to enable continuity of essential services—or critical functions—during periods of stress on critical infrastructure systems. This type of approach generally emphasizes criticality as a characteristic that varies over time or situational context rather than as a static or fixed descriptor of a particular asset. Critical infrastructure inventory programs that reflect this approach may expand the scope of data collection to include any and all assets within a given sector that might become useful in emergency planning or contingency situations. (See **text box** below on "Homeland Infrastructure Foundation-Level Data.") Information-sharing and incident reporting requirements are often similarly expansive, covering a broad range of critical infrastructure entities. Available data can then be used as needed by public and private-sector entities to assess risk to continuity of critical functions and identify alternative means of maintaining these functions when contingencies arise.

A decade after the 9/11 attacks, federal policy increasingly emphasized CIR approaches. Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience," issued on February 12, 2013, by President Obama, marked a departure from the asset-centric CIP approaches of the preceding decade set forth in HSPD-7, which it superseded.[33] As its title implies, PPD-21 framed the national critical infrastructure enterprise in terms of resilience, de-emphasizing asset-identification and protection approaches. In contrast with HSPD-7, it did not set forth any specific requirements for federal agencies to identify critical infrastructure assets. Rather, it emphasized "all-hazards" 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," PPD-21 stated. "Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery." It tasked the Secretary of Homeland Security with making holistic analyses of key interdependencies between critical infrastructure sectors and other risks, and facilitating public-private partnerships for risk management, among other requirements.

[32] Gregory M. Chabon et al., "Shelter in Place Orders: Are You an 'Essential Business'?," *National Law Review*, vol. XVI, no. 48 (March 23, 2020), https://natlawreview.com/article/shelter-place-orders-are-you-essential-business.

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

Homeland Infrastructure Foundation-Level Data

The primary critical infrastructure interagency database using the critical infrastructure resilience approach is known as Homeland Infrastructure Foundation-Level Data (HIFLD).[34] Four lead agencies—the Department of Homeland Security (DHS), the Department of Defense,[35] the National Geospatial-Intelligence Agency, and the U.S. Geological Survey—compile data gleaned from outreach to public and private-sector partners and make the data available to eligible law enforcement, emergency management, and other organizations at all levels of government.

HIFLD is composed of hundreds of data "layers" that encompass nearly every conceivable category of asset relevant to homeland security functions and are curated by designated partner agencies, or "stewards." Layers include assets considered critical under any definition that are essential to supporting lifeline critical infrastructure functions of energy, communications, transportation systems, and water and wastewater systems. 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 critical infrastructure policy decisions—for example, truck driving schools, express shipping facilities, and cruise ship terminals.

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 National Critical Infrastructure Prioritization Program list, it does not elevate the status of specific systems and assets in ways that directly support official functions of federal oversight, regulation, and administration. However, it is widely used to inform preparedness and incident management activities of federal, state, local, tribal, and territorial agencies. HIFLD also provides public domain data for community preparedness, resilience, and research through the HIFLD Open service for nongovernmental users. In 2025, DHS discontinued the HIFLD Open service, raising concerns in some quarters that nonfederal stakeholders would face greater difficulty in accessing relevant data to support the critical infrastructure enterprise before, during, and after emergencies.[36]

National Critical Functions

Shortly after its founding in 2018, CISA established a set of 55 national critical functions (NCFs) as a framework for cross-sector risk analysis. CISA defined NCFs as critical-infrastructure-enabled functions "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."[37] Although the language used in this formulation echoes that of the statutory definition of critical infrastructure, it has a CIR orientation.

CISA organizes NCFs within four broad areas: connect, distribute, manage, and supply. Each area includes a broad range of activities (see **Appendix B**). CISA uses the framework to guide analyses of complex interdependencies between infrastructure systems and identification of assets that enable continuity of critical functions. According to CISA, "By viewing risk through a

[34] For more information, see DHS, Geospatial Management Office, "Homeland Infrastructure Foundation-Level Data (HIFLD)," September 4, 2025, https://www.dhs.gov/gmo/hifld.

[35] The Department of Defense is currently "using a secondary Department of War designation," under E.O. 14347 of September 5, 2025, "Restoring the United States Department of War," 90 *Federal Register* 43893, September 10, 2025, https://www.federalregister.gov/documents/2025/09/10/2025-17508/restoring-the-united-states-department-of-war.

[36] Adam Simmons, "The Rise, Power, and Uncertain Future of America's Open Infrastructure Data," *Project Geospatial*, September 8, 2025, https://projectgeospatial.org/geospatial-frontiers/the-rise-power-and-uncertain-future-of-americas-open-infrastructure-data.

[37] In 2019, the Cybersecurity and Infrastructure Security Agency (CISA) promulgated the National Critical Function (NCF) set to improve methods for infrastructure risk assessment and enable better collaboration across multiple critical infrastructure sectors. See CISA, "National Critical Functions Set," https://www.cisa.gov/national-critical-functions-set (hereinafter CISA NCF Set). The definition of national critical functions parallels the statutory definition of critical infrastructure given in the USA PATRIOT ACT (P.L. 107-56). 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" (§1016(e)).

functional lens, we can ultimately add resilience and harden systems across the critical infrastructure ecosystem in a more targeted, prioritized, and strategic manner. This allows for a more holistic analysis of risks and associated dependencies that may have cascading impacts within and across sectors."[38]

Cyber Incident Reporting for Critical Infrastructure Act of 2022 and Identification of Critical Infrastructure Entities

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA; P.L. 117-103, Division Y) directed CISA to create a mandatory cyber incident and ransomware reporting program that covers certain critical infrastructure entities across all sectors. The focus on critical infrastructure entities—rather than individual assets—suggests a broader emphasis on CIR approaches to CISR. The proposed rule—issued in April 2024—applied to certain "critical infrastructure entities" that have significant operations within one or more critical infrastructure sectors.[39] These entities would be covered by the mandatory reporting requirements if they exceed a certain size threshold of number of employees or revenue—justified on the grounds that larger entities are more likely to be targeted by malicious cyber actors and that such attacks are likely to have more severe consequences, including disruption of critical infrastructure.

The proposed rule contained sector-specific provisions that provided risk-based criteria for defining covered entities under the statute.[40] As written, the proposed rule was agnostic regarding risk to specific systems and assets—a departure from CIP-centric approaches that defined and managed risk at the asset level. Instead, the proposed rule would focus on reducing risk to critical infrastructure sectors as a whole. Therefore, critical infrastructure entities may be covered by the regulation if their ability to deliver critical services within a sector might be compromised by certain cyber incidents, even if they do not operate systems and assets that meet the statutory threshold of criticality as defined in CIPA.

Potentially covered entities would be expected to "self-identify" as members of the critical infrastructure sector "that most closely align[s] with the line of activities in which the entity is engaged."[41] Further, critical infrastructure entities in certain sectors would be subject to additional criteria specific to that sector. Some examples include suppliers that provide certain information technology (IT) products to the federal government and critical infrastructure entities in the Health Care and Public Health sector that manufacture certain drugs or medical devices. In February 2026, DHS announced a series of town hall meetings to allow stakeholders additional time to comment on the proposed rule and provide "specific, actionable improvements that CISA could implement in the final rule to clarify or reduce burden of CIRCIA's regulatory requirements while enhancing the federal government's visibility into the cyber threat landscape for critical infrastructure sectors."[42]

---

[38] CISA, "National Critical Functions," https://www.cisa.gov/topics/risk-management/national-critical-functions.

[39] DHS, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements," 89 *Federal Register* 23644, April 4, 2024, https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements (hereinafter CIRCIA proposed rule on reporting requirements).

[40] CIRCIA proposed rule on reporting requirements.

[41] CIRCIA proposed rule on reporting requirements.

[42] DHS, "Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Rulemaking; Town Hall Meetings," 91 *Federal Register* 6794, February 13, 2026, https://www.federalregister.gov/documents/2026/02/13/2026-02948/cyber-incident-reporting-for-critical-infrastructure-act-circia-rulemaking-town-hall-meetings.

National Security Memorandum 22

National Security Memorandum 22 (NSM-22), "Critical Infrastructure Security and Resilience," was issued by the Biden Administration in April 2024, superseding PPD-21—the 2013 directive with the same title issued by the Obama Administration (see "Resilience-Based Approaches to Risk Management" section).[43] PPD-21 contained no specific asset identification and prioritization requirements for federal agencies—an apparent reflection of an emerging policy consensus favoring a focus on CIR over CIP approaches. By contrast, NSM-22 placed comparatively greater emphasis on CIP and management of asset-level risk than PPD-21 while continuing to emphasize many of the CIR themes in PPD-21. Thus, it demonstrated that CIP and CIR approaches frequently coexist, even though one or the other may receive comparatively greater emphasis based on policy context and Administration priorities.[44]

NSM-22 established the Director of CISA as the National Coordinator for the Security and Resilience of Critical Infrastructure—reaffirming earlier designations made in CISA's founding statute and by the Secretary of Homeland Security. It required the National Coordinator to identify Systemically Important Entities (SIE)—that is, "organizations that own, operate, or otherwise control critical infrastructure that is prioritized based on the potential for its disruption or malfunction to cause nationally significant and cascading negative impacts to national security (including national defense and continuity of Government), national economic security, or national public health or safety."[45] The directive did not specify a specific methodology for SIE identification, instead delegating this task to designated federal agencies, assisted by other federal departments and "non-federal entities, as appropriate."

The SIE requirement was an extension of a 2013 presidential cybersecurity directive, which directed the Secretary of Homeland Security to identify high-risk critical infrastructure assets potentially vulnerable to cyberattacks on an annual basis through consultations with relevant federal agencies and other public and private-sector stakeholders using established coordination mechanisms.[46] According to NSM-22, the SIE list "shall inform prioritization of Federal activities," including application of "adequate risk management requirements" and "provision of risk mitigation information and other operational resources" to critical infrastructure entities. Thus, critical infrastructure asset identifications and the resulting SIE designations would drive much of the federal government's coordination of the national critical infrastructure enterprise under NSM-22.

Federal Organization for Critical Infrastructure Risk Management

Federal organization for critical infrastructure risk management has changed significantly in response to evolving threats and the accompanying maturation of the homeland security enterprise. Four distinct periods of development identified by CRS are covered below: the initial

[43] White House, "National Security Memorandum on Critical Infrastructure Security and Resilience," National Security Memorandum 22 (NSM-22), April 30, 2024, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/ (hereinafter NSM-22).

[44] For more information on NSM-22, see CRS In Focus IF12716, *The 2024 National Security Memorandum on Critical Infrastructure Security and Resilience*, by Brian E. Humphreys.

[45] NSM-22.

[46] E.O. 13636 of February 12, 2013, "Improving Critical Infrastructure Cybersecurity," 78 *Federal Register* 11739, February 19, 2013. Entities controlling designated high-risk assets are commonly referred to as "Section 9 entities," after the section in E.O. 13636 that contained the requirement.

policy development and coordination initiatives of the late 1990s, the post-9/11 reorganization of federal government to counter terrorist threats to infrastructure, the transition to the all-hazards resilience framework for infrastructure security based on voluntary public-private partnerships, and the creation of CISA.

From the 1990s to the Homeland Security Act of 2002

Federal attention to critical infrastructure 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 President's 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.[47] 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.[48]

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 the duties of the position 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 terrorist threats to national security as well as early efforts to implement PDD-63. The Gilmore Commission, as it was known, submitted a report to Congress and the Clinton Administration in December 2000 titled *Toward a National Strategy for Combating Terrorism*. The report noted that implementation of PDD-63 was incomplete and that the nascent CIP enterprise had developed only fitfully since PDD-63 was signed in 1998.[49] Specifically, the Gilmore Commission found the following:

- 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 Counter-Terrorism 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 critical infrastructure threat and vulnerability assessments, warning and response coordination, and law enforcement investigation and response activities, had

[47] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*, October 1997, p. i.

[48] PDD-63.

[49] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, *Toward a National Strategy for Combating Terrorism*, second annual report, December 15, 2000, 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 Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (P.L. 105-261).

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, CIP. Policy initiatives that had previously languished became matters of 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 Office of National Drug Control Policy.[50] 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 the Department of Defense in 1998 to study 21st century security issues, known as the Hart-Rudman Commission.[51] 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 (P.L. 107-296) generally reflected the approach that the Hart-Rudman Commission had advocated for.

The Homeland Security Act of 2002 created DHS and transferred many infrastructure security functions to DHS that previously had been regarded as properly belonging to the 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.[52] 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.[53] Although several long-established agencies, such as the U.S. 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 counterterrorism-focused approach represented a change from previous infrastructure policy. Previous Administrations had regarded CIP as only tangentially related to counterterrorism

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

[51] The commission was formally known as the U.S. Commission on National Security/21st Century but was commonly referred to as the "Hart-Rudman Commission" after its chairmen, former Sens. Gary Hart and Warren Rudman.

[52] DHS, "GAO High-Risk Management," October 18, 2023, https://www.dhs.gov/gao-high-risk-management. Also see GAO, *Homeland Security: Title III of the Homeland Security Act of 2002*, GAO-02-927T, July 9, 2002, https://www.gao.gov/assets/110/109473.pdf.

[53] The National Infrastructure Protection Center was among the many entities transferred.

functions of government before 9/11. The Office of Management and Budget (OMB) stated in a 2001 report to Congress on federal counterterrorism programs that "CIP is a separate but related mission."[54] OMB justified this distinction on the grounds that infrastructure risks were diverse and included many hazards beyond terrorism, such as equipment failure, human error, weather and natural disasters, and criminal activity. OMB wrote, "This year's report focuses on combating terrorism, mentioning CIP efforts only where they directly impact the combating terrorism mission."[55] That direct impact, according to budget estimates in the 2001 report, was negligible. CIP funding that overlapped counterterrorism funding amounted to less than 0.5% of the total CIP funding of $2.6 billion requested by the George W. Bush Administration for FY2002.[56]

The terrorist attacks of 9/11 changed the budget picture significantly, as seen in OMB's *2003 Report to Congress on Combating Terrorism*.[57] 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 FY2004 Bush Administration request for CIP funding across all agencies was $12.2 billion, an increase of more than 450% over the FY2002 request—the Administration's final pre-9/11 request—and included 28 federal entities outside the newly created DHS.[58] The 2003 OMB report did not provide a separate estimate of the proportion of the CIP-related budget that overlapped counterterrorism funding, 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.[59]

Evolution of Critical Infrastructure 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.[60] 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—DHS.[61]

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

---

[54] Office of Budget and Management (OMB), *Annual Report to Congress on Combating Terrorism*, August 2001, p. 2, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/legislative/nsd_annual_report2001.pdf (hereinafter OMB 2001 Terrorism Report).

[55] OMB 2001 Terrorism Report, p. 2.

[56] OMB 2001 Terrorism Report, p. 6.

[57] OMB, *2003 Report to Congress on Combating Terrorism*, September 2003, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/legislative/2003_combat_terr.pdf (hereinafter OMB 2003 Terrorism Report).

[58] OMB 2003 Terrorism Report, p. 13.

[59] OMB 2001 Terrorism Report, p. 37.

[60] Letter from Sen. Joe Lieberman to Tom Ridge, Homeland Security Advisor, March 19, 2002, https://www.hsgac.senate.gov/media/dems/lieberman-seeks-answers-from-ridge-on-homeland-security-improvements/. As Chairman of the Senate Committee on Homeland Security and Governmental Affairs, Sen. Lieberman introduced legislation to create DHS. Also see the letter from the President in White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003.

[61] OMB 2003 Terrorism Report, p. 7.

aftermath of the attacks, 46% of Americans surveyed by Gallup named terrorism as the most important problem facing the United States.[62] By the second half of 2005, the percentage hovered between 6% and 8%.[63] This broad trend has continued, with periodic upticks caused by high-profile incidents. For the last six months in 2024, 1% or fewer of respondents to the Gallup survey listed terrorism as the most important national problem.[64]

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 beside terrorism. Issues of equipment failure, human error, weather and natural disasters, and criminal activity highlighted in the pre-9/11 OMB report reemerged as national-level policy concerns.[65]

Transition to All-Hazards Approach

In 2006, the Critical Infrastructure Task Force of the Homeland Security Advisory Council (HSAC) 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.[66] 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 encouraged resilience as well as protection.[67] 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.[68] 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."[69] Examples of threats and hazards included natural disasters (specifically, Hurricane Katrina), cyberattacks, the expansion of transnational crime, and contagious diseases.[70]

---

[62] Jim Norman, "How High Will Terrorism Concerns Rise, How Long Will They Last?," *Gallup*, June 15, 2016, https://news.gallup.com/poll/192713/high-terrorism-concerns-rise-long-last.aspx (hereinafter Gallup Terrorism Survey). Survey data on immediate post-9/11 attitudes from October 2001.

[63] Gallup Terrorism Survey.

[64] Gallup, "Most Important Problem," accessed January 10, 2025, https://news.gallup.com/poll/1675/most-important-problem.aspx.

[65] OMB 2001 Terrorism Report.

[66] Homeland Security Advisory Council, *Report of the Critical Infrastructure Task Force*, January 2006, p. 4, https://www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf.

[67] 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.

[68] P.L. 107-296.

[69] DHS, *Quadrennial Homeland Security Review Report*, February 1, 2010, p. vii, https://www.dhs.gov/sites/default/files/publications/2010-qhsr-report.pdf. See P.L. 107-296, as amended by P.L. 115-387, §707.

[70] Transnational crime risks to critical infrastructure functions may include ransomware attacks and other cyber-related crimes, as well as intentional supply chain corruption, counterfeiting, theft, and extortion. For examples in the Food and Agriculture sector, see "The Role of Transnational Criminal Organizations" section in CRS Report R48094, *Foreign Ownership, Control, and Influence (FOCI) Risks in the Food and Agriculture Sector*, by Brian E. Humphreys.

Subsequent QHSRs continued the general trend toward an approach to risk management that encompassed an increasing range of hazards beyond terrorism over time.[71]

Role and Organization of CISA

The Cybersecurity and Infrastructure Security Agency Act of 2018 (CISA Act; P.L. 115-278) created the eponymous agency as an operational component of DHS to take over the functions previously carried out by the National Protection and Programs Directorate.[72] The law directed CISA to lead cybersecurity and infrastructure security programs, in coordination with federal agencies and CISR stakeholders, to secure federal IT systems, to conduct critical infrastructure risk assessments and planning activities, and to provide technical assistance to infrastructure owner-operators, among other provisions.

The creation of a dedicated agency for infrastructure security elevated critical infrastructure risk management as an area of policy focus. The CISA Act directed CISA to establish an organizational structure that would include three divisions—Cybersecurity, Infrastructure Security, and Emergency Communications.[73] CISA established three additional operational divisions focused on integration of agency functions and stakeholder engagement.[74]

The National Risk Management Center (NRMC) "identifies the most significant risks in all 16 critical infrastructure sectors and promotes risk reduction activities to improve the security and resilience of critical infrastructure now and into the future."[75] According to CISA, the NRMC "provides vital analytic and strategic support to mitigate risk to the cyber and physical infrastructure Americans rely on every day."[76] The Integrated Operations Division of CISA provides CISA with a nexus to the federal intelligence community and operates CISA Central, which provides a centralized information hub for external critical infrastructure stakeholders.[77] The Stakeholder Engagement Division facilitates CISA's various activities as the primary federal coordinator of voluntary public-private partnerships for infrastructure security and resilience as set forth in NSM-22 and other policy guidance.[78]

CISA Regulatory Authorities

The creation and maturation of CISA coincided with a trend in the executive branch toward more assertive use of federal authorities to advance resilience goals, such as increased private-sector investments in infrastructure resilience, reporting of cyber and physical security incidents, and

[71] DHS *Quadrennial Homeland Security Review Report*, February 1, 2010, p. 13. For example, the 2014 Quadrennial Homeland Security Review cited the 2010 Deepwater Horizon oil spill—an industrial accident caused in part by negligence—as a homeland security hazard. See DHS, *The 2014 Quadrennial Homeland Security Review*, June 18, 2014, p. 5, https://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

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

[73] The heads of the Cybersecurity and Infrastructure Security divisions are appointed by the President without the advice or consent of the Senate.

[74] CISA, "Organizational Chart," March 18, 2025, https://www.cisa.gov/sites/default/files/2025-03/CISA-Org-Chart-03182025-508.pdf.

[75] CISA, "National Risk Management Center," https://www.cisa.gov/about/divisions-offices/national-risk-management-center.

[76] CISA, "National Risk Management Center," https://www.cisa.gov/about/divisions-offices/national-risk-management-center.

[77] CISA, "Integrated Operations Division," https://www.cisa.gov/about/divisions-offices/integrated-operations-division.

[78] CISA, "Stakeholder Engagement Division," https://www.cisa.gov/about/divisions-offices/stakeholder-engagement-division.

engagement in public-private partnerships. Since CISA's creation, Congress has given the agency additional authorities to enable greater federal oversight and control of the national CISR enterprise.

The Federal Information Security Modernization Act of 2014 (FISMA; P.L. 113-283) authorizes DHS to issue binding operational directives (BODs) for federal agencies to implement for the protection and security of federal information and IT systems, which are part of the Government Services and Facilities critical infrastructure sector.[79] BODs typically cover device, configuration, or software vulnerabilities that federal agencies must remediate on their computer systems.[80] DHS acts through CISA to exercise this authority.

In 2021, Congress provided administrative subpoena powers to CISA, which the agency had sought for several years. Under authorities enacted in the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY2021 NDAA; P.L. 116-283), CISA may issue administrative subpoenas to internet service providers to obtain subscriber information if such information is needed to identify at-risk critical infrastructure systems connected to the internet. In such cases, CISA would notify critical infrastructure owners of the relevant security risks.

In 2022, Congress designated CISA as the implementing agency for CIRCIA (see "Cyber Incident Reporting for Critical Infrastructure Act of 2022 and Identification of Critical Infrastructure Entities" section). A July 2024 GAO report found that CISA had implemented 13 of 25 CIRCIA implementation requirements.[81] In June 2025, the House Committee on Appropriations directed CISA to provide it with a briefing on a plan to spend appropriated funds for implementation of statutory requirements.[82]

A notable exception to the trend toward expanding federal authority and oversight over critical infrastructure is CISA's Chemical Facility Anti-Terrorism Standards (CFATS) program to prevent terrorist exploitation of the chemical industry, which was allowed to sunset in July 2023. However, even in this case, the congressional record suggested significant support in the 118th Congress for reauthorizing the program and maintaining CISA regulatory authority. The House passed a bill (H.R. 4470) on a 409-1 vote to extend the authorization for two years. A companion Senate bill (S. 2499) did not advance past introduction, and a motion to consider the House-passed bill was blocked in the Senate.[83]

CISA encouraged previously covered chemical facilities to maintain existing security measures and noted the availability of its resources for adoption of voluntary best practices under the ChemLock initiative, which provides a toolkit of on-site assessments and assistance, exercise packages, on-demand training, and online informational guidance.[84] In addition, CISA Chemical Security Inspectors (CSIs), formerly tasked with enforcing regulatory compliance with CFATS requirements, continued to be available to assist chemical facilities with making safety and

[79] 44 U.S.C. §3553. For a sector overview, see CISA, "Government Services and Facilities Sector," https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/government-services-facilities-sector.

[80] CISA, "Cybersecurity Directives," accessed September 29, 2025, https://www.cisa.gov/news-events/directives.

[81] GAO, *Critical Infrastructure Protection: DHS Has Efforts Underway to Implement Federal Incident Reporting Requirements*, GAO-24-106917, July 30, 2024, https://www.gao.gov/products/gao-24-106917.

[82] U.S. Congress, House Committee on Appropriations, Subcommittee on Homeland Security, *Department of Homeland Security Appropriations Bill, 2026*, report to accompany H.R. 4213, 119th Cong., 1st sess., H.Rept. 119-173, June 26, 2025, pp. 69-70, 75.

[83] Sen. Gary C. Peters and Sen. Rand Paul, "National Defense Authorization Act for Fiscal Year 2024," debate in the Senate, *Congressional Record*, vol. 169, part 1 (July 26, 2023), pp. S3572-S3574.

[84] CISA, "ChemLock," https://www.cisa.gov/resources-tools/programs/chemlock.

security improvements on a voluntary basis. CISA's FY2026 budget justification proposed phasing out all CSI positions and the chemical security program.[85]

CISA Services for Critical Infrastructure Sectors

CISA also has made several other types of security advisors available to various infrastructure sectors on a voluntary basis.[86] Cyber Security Advisors and Protective Security Advisors from CISA regional offices conduct outreach to infrastructure operators and other stakeholders to advise and assist on various security matters. Emergency Communications Coordinators "support emergency communications interoperability by offering training, tools, and workshops, and provide coordination and support in times of threat, disruption, or attack" to stakeholders in the Emergency Services critical infrastructure sector. Election Security Advisors are specialists in elections-related "processes, procedures, and technologies" and work with state and local election officials to coordinate technical assistance from CISA on cyber and physical security matters affecting the Election Infrastructure critical infrastructure subsector.[87]

In addition to services provided directly by security advisors, CISA has offered a range of cybersecurity and physical-security-related services at no cost for industries that own or operate critical infrastructure. These services may include intrusion monitoring, vulnerability scanning, threat tracking and reporting, and self-assessment tools, among others. For example, the Common Vulnerabilities and Exposures (CVE) program funded by CISA provides a publicly available catalog of known cybersecurity vulnerabilities to cybersecurity partners.[88] Other resources include the CISA Gateway portal, which "serves as the single interface through which CISA partners can access a large range of integrated infrastructure protection tools and information to conduct comprehensive vulnerability assessments and risk analysis."[89]

Media sources in April and May 2025 reported numerous resignations of senior leaders and a wave of continuing departures that the sources anticipated could eventually affect up to one-third of the CISA workforce.[90] At a May 2025 industry event, then-Secretary of Homeland Security Kristi Noem said cybersecurity was a top priority for the Trump Administration but that "we need to put CISA back on mission," focused on critical infrastructure and national defense.[91] Media

---

[85] DHS, *Cybersecurity and Infrastructure Security Agency Budget Overview: Fiscal Year 2026 Congressional Justification*, June 9, 2025, p. O&S – 18, https://www.dhs.gov/sites/default/files/2025-06/25_0613_cisa_fy26-congressional-budget-justificatin.pdf (hereinafter CISA FY2026 budget justification).

[86] CISA, "Security Advisors," https://www.cisa.gov/about/regions/security-advisors.

[87] CISA, *Critical Infrastructure Outreach: Fiscal Year 2024 Report to Congress*, October 23, 2024, p. 20, https://www.dhs.gov/sites/default/files/2024-12/2024_1023_cisa_critical_infrastructure_outreach.pdf.

[88] See Common Vulnerabilities and Exposures, "Overview: About the CVE Program," https://www.cve.org/About/Overview.

[89] See CISA, "CISA Gateway," https://www.cisa.gov/resources-tools/services/cisa-gateway. Access to the portal is restricted to partners who complete required training and are certified to access protected critical infrastructure information (see "Incentives for Private Sector Participation" section).

[90] Eric Geller, "CISA Loses Nearly All Top Officials as Purge Continues," *Cybersecurity Dive*, May 27, 2025, https://www.cybersecuritydive.com/news/cisa-senior-official-departures/748992/; Chris Riotta, "White House Proposes $500 Million Cut to CISA," May 2, 2025, *GovInfoSecurity*, https://www.govinfosecurity.com/white-house-proposes-500-million-cut-to-cisa-a-28216; and Maggie Miller and John Sakellariadis, "CISA's Mass Layoff Plan May Be On Pause After Hundreds of Staff Voluntarily Resigned," *Politico*, May 13, 2025, https://subscriber.politicopro.com/article/2025/05/cisa-layoffs-hundreds-deferred-resignation-offers-00346299. The reports suggest that departures were in response to deferred resignation offers, unilateral restructuring by executive branch entities, and declining morale.

[91] David Jones, "DHS Secretary Vows to Refocus CISA, Saying It Strayed from Mission," *Cybersecurity Dive*, April 30, 2025, https://www.cybersecuritydive.com/news/dhs-secretary-vows-to-refocus-cisa-saying-it-strayed-from-mission/746739/.

reports in September 2025 quoted state cybersecurity officials who reported diminished support from CISA regional offices, cybersecurity advisors, and certain federally assisted ISACs, which they feared might leave critical infrastructure in their states more vulnerable to cyberattacks.[92] Other reports suggested that the CVE program was slated to be defunded in April 2025 before "overwhelming support" from industry and government partners led to renewal of the program contract with MITRE Corporation.[93]

Public-Private Partnerships

Although much of the nation's critical infrastructure is privately owned, the public may be put at risk if these privately owned systems fail (see **text box** below on "Public Impacts of Private Business Risk"). Management of critical infrastructure risk to national security, economic security, and public health 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.[94] Under this model, critical infrastructure owner-operators, not the government, have ultimate responsibility for assessing and mitigating risk to their own assets. At the same time, Congress has directed executive branch agencies to assess and manage risk at the national level. Infrastructure risk management has been structured under this framework as a largely collaborative endeavor between the public and private sectors reliant on incentives, information sharing, and voluntary investments in security.

[92] Maggie Miller, "States Send Out the 'Bat Signal' for Help Responding to Cyber Threats Amid Federal Cuts," *Politico*, September 26, 2025, https://subscriber.politicopro.com/article/2025/09/states-cyber-response-federal-cuts-00582295.

[93] Maggie Miller, "Cyber Agency Restores Funding to Major Vulnerability Tracker Hours Before Its Closure," *PoliticoPro*, April 16, 2025, https://subscriber.politicopro.com/article/2025/04/cyber-agency-restores-funding-to-major-vulnerability-tracker-hours-preventing-its-closure-00293506.

[94] PDD-63.

Public Impacts of Private Business Risk

Businesses protect their productive assets from theft, destruction, and malicious exploitation to prevent losses and ensure continuity of operations.[95] Private business risks are typically not a matter of public concern as long as consequences of any service disruption are localized and 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 of the year, leading to a much wider crisis. The Michigan governor issued an urgent plea via the Integrated Public Alert and Warning System (IPAWS) for residents to turn their thermostats down in order to avoid a catastrophic 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.[96] 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. Consumers Energy's own investigation found that equipment was properly maintained but that a routine venting process "became hazardous" because of unanticipated effects of high winds.[97]

Critical Infrastructure Sectors

The federal government established critical infrastructure sectors as an organizing framework for voluntary public-private partnerships for risk management with self-identified owner-operators. The purpose of such partnerships has been to create channels for voluntary exchange of information about infrastructure-related risks between the public and private sectors in order to improve security and resilience within each sector. Public-private partnership activities are generally nonregulatory in nature but may inform certain regulatory activities or develop in tandem with them (see "The Relationship Between Voluntary Partnerships and Federal Regulation" section). Currently, there are 16 designated critical infrastructure sectors as set forth in presidential directives (see **Table 1**).[98]

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

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

[97] Consumers Energy released results of an internal investigation on April 5, 2019, finding it was not at fault for the incident. See Consumers Energy, "Statement from Consumers Energy as the Company Submits Report on the Cause of the January Ray Compressor Fire," April 5, 2019, 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. The local regulator, the Michigan Public Service Commission, completed a report in January 2020. For a report summary and details of related proceedings, see Michigan Public Service Commission, *In the matter, on the Commission's Own Motion, to Commence an Investigation into a January 30, 2019 Fire at CONSUMERS ENERGY COMPANY's Ray Compressor Station in Macomb County*, Case No. U-20463, May 20, 2020, https://adms.apps.lara.state.mi.us/Mpsc/ViewCommissionOrderDocument/25523.

[98] As of this date of this report, current guidance is set forth in NSM-22, issued by the Biden Administration in April 2024.

Table 1. Critical Infrastructure Sectors

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
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 research and development; designs, manufactures, and integrates systems; and maintains depots and services military weapon systems, subsystems, components, subcomponents, or parts.	DOD
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 (1) electricity and (2) oil and natural gas.	DOE
Financial Services	Provides critical financial utilities and services that support investment, credit and financing, and insurance.	Treasury
Food and Agriculture	Produces, processes, distributes, and serves food.	USDA
Government Facilities	Includes a wide variety of nearly 900,000 constructed assets owned or leased by federal, state, local, tribal, or territorial governments and used to provide the full range of government services.	DHS and GSA
Health Care and Public Health	Provides essential health care and public health services. Conducts related research and development, manufactures pharmaceuticals and other essential medical supplies, and manages supply chains required for care delivery.	HHS
Information Technology	Produces information technology and includes 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, buses, and mass transit	DHS and DOT
Water and Wastewater Systems	Provides drinking water and treatment of wastewater.	EPA

Source: Department of Homeland Security (DHS), *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 2013, https://www.nist.gov/system/files/documents/cybercommission/-DHS-_National_Infrastructure_Protection_Plan_-NIPP.pdf; sector-specific plans (for archived examples, see Cybersecurity and Infrastructure Security Agency, "2015 Sector-Specific Plans," https://www.cisa.gov/2015-

sector-specific-plans); and Government Accountability Office, *Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption*, GAO-18-211, February 2018, https://www.gao.gov/assets/gao-18-211.pdf.

Notes: DOD = Department of Defense; DOE = Department of Energy; DOT = Department of Transportation; GSA = General Services Administration; HHS = Department of Health and Human Services; Treasury = Department of the Treasury; EPA = Environmental Protection Agency; USDA = U.S. Department of Agriculture.

Public-Private Partnership Coordination Bodies

CISA has overall responsibility for coordination of public-private partnership programs and activities across all critical infrastructure sectors as the National Coordinator for CISR. These programs have provided forums for coordination on CISR activities that affected areas of mutual concern, such as threat reporting, risk assessments, promulgation of best practices, and other forms of information sharing. The Federal Senior Leadership Council (FSLC) has been the interagency coordination body that provides "national and cross-sector guidance and priorities" to SRMAs. It is composed of senior officials from federal departments and agencies "with responsibilities for critical infrastructure security and resilience."[99] It is the primary federal entity responsible for implementation of federal CISR policy, such as NSM-22 and any successor documents. It is cochaired by the CISA Director and a senior official from one of the non-CISA SRMAs.[100]

SRMAs lead public-private partnership coordination bodies, which have been organized under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) first established in 2006 by DHS under the authorities of the Homeland Security Act of 2002. The CIPAC Charter was renewed several times since then, most recently in 2024.[101] Under certain circumstances, CIPAC provided designated public-private coordinating bodies with legal exemption from Federal Advisory Committee Act (FACA) provisions for open meetings, chartering, public involvement, and reporting in order to facilitate multilateral discussions between critical infrastructure stakeholders on sensitive topics relating to infrastructure security.[102] Therefore, CIPAC provided the legal and institutional framework for SRMAs and other relevant federal agencies to engage private-sector stakeholders through the NIPP partnership structure. This process was used to develop consensus policy advice and recommendations for DHS and other relevant agencies.

The partnership structure was more flat than hierarchical and was realized in multiple formats, including symposia, research collaborations, working groups, policy deliberations, and emergency preparedness and response activities. By design, participation in these activities has often crossed organizational lines and included governmental and nongovernmental stakeholders. Increasingly, partnership activities have included representatives from multiple critical infrastructure sectors because of recognition of the interdependencies inherent in complex critical

[99] Federal Senior Leadership Council (FSLC), *Charter*, November 7, 2024, pp. 1, 2, https://www.cisa.gov/sites/default/files/2024-11/fslc-charter-2024-508.pdf (hereinafter FSLC Charter).

[100] FSLC Charter, p. 4.

[101] DHS, "Notice of the Renewal of the Critical Infrastructure Partnership Advisory Council Charter," 89 *Federal Register* 92699, November 22, 2024, https://www.federalregister.gov/documents/2024/11/22/2024-27340/notice-of-the-renewal-of-the-critical-infrastructure-partnership-advisory-council-charter.

[102] Exemptions from the Federal Advisory Committee Act (FACA; 5 U.S.C. Chapter 10) are made by the Secretary of Homeland Security 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.

infrastructure systems and the general policy trend favoring system resilience over asset protection.[103]

On March 13, 2025, DHS terminated CIPAC authorities in accordance with E.O. 14217 of February 19, 2025, "Commencing the Reduction of the Federal Bureaucracy."[104] This action does not—in and of itself—terminate public-private partnerships for CISR that developed in recent decades. However, it does eliminate previously existing provisions for confidential deliberations. Some observers have voiced concerns that this will diminish information sharing between private-sector entities and government agencies that enables cybersecurity and infrastructure security collaboration, but others have expressed optimism that CIPAC might be replaced with a better framework for collaboration.[105] Media reports in early 2026 indicated that DHS was finalizing plans for a replacement, to be known as the Alliance of National Councils for Homeland Operational Resilience (ANCHOR), which would modify the previous structure and liability protections that existed under the CIPAC framework. According to these reports, the new structure would offer "wider latitude" for open meetings and records of stakeholder engagements.[106]

Government Coordinating Councils

Each of the 16 designated critical infrastructure sectors has had its own Government Coordinating Council (GCC) and Sector Coordinating Council (SCC), which were organized under CIPAC auspices between 2006 and March 2025. GCCs are made up of state, local, tribal, and territorial (SLTT) and federal agencies and, according to the NIPP, enable "interagency, intergovernmental, and cross-jurisdictional coordination" on infrastructure issues of common concern.[107] Each GCC has been led by a designated SRMA. Statutory roles and responsibilities for SRMAs were elaborated in the FY2021 NDAA (see **text box** below on "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY2021 NDAA)"). DHS (acting through CISA) led or co-led 10 of the 16 GCCs as the SRMA. Other SRMAs include the Environmental Protection Agency, the General Services Administration, and the Departments of Agriculture, Defense, Energy, Health and Human Services, Transportation, and the Treasury. (See **Table 1** for description of critical infrastructure sectors and SRMAs, and see **Appendix C** for a visualization of critical infrastructure partnership structure.) SRMAs have leveraged 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. According to

[103] Organisation for Economic Co-operation and Development (OECD), *Good Governance for Critical Infrastructure Resilience*, OECD Reviews of Risk Management Policies, 2019, p. 3, https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/good-governance-for-critical-infrastructure-resilience_7d5a9993/02f0e5a0-en.pdf (hereinafter OECD Risk Management Review).

[104] DHS, "Notice of Termination of Discretionary Federal Advisory Committees," 90 *Federal Register* 11995, March 13, 2025, https://www.federalregister.gov/documents/2025/03/13/2025-04011/notice-of-termination-of-discretionary-federal-advisory-committees.

[105] Eric Geller, "'Suspended Animation': U.S. Government Upheaval Has Frayed Partnerships with Critical Infrastructure," *Cybersecurity Dive*, June 25, 2025, https://www.cybersecuritydive.com/news/critical-infrastructure-cybersecurity-partnerships-disruption-trump-government-industry/751589/; and Sam Sabin, "Cyber Council's Demise Shakes Public-Private Sector Trust," *Axios*, March 18, 2025, https://www.axios.com/2025/03/18/dhs-cisa-cyber-council-industry-trust.

[106] Derek B. Johnson, "Sources: DHS Finalizing Replacement for Disbanded Critical Infrastructure Security Council," *CyberScoop*, January 14, 2026, https://cyberscoop.com/dhs-anchor-cipac-replacement-critical-infrastructure-cybersecurity-liability-protections/.

[107] DHS, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 2013, p. 12, https://www.nist.gov/system/files/documents/cybercommission/-DHS-_National_Infrastructure_Protection_Plan_-NIPP.pdf (hereinafter NIPP 2013).

media reports, then-Secretary Noem said during an April 2025 public appearance in San Francisco that she would reinstate CIPAC to "bring more people to the table and be much more action oriented."[108]

William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (FY2021 NDAA)

The FY2021 NDAA (P.L. 116-283, §9001) established new qualifications for the CISA Director position established in 2018. Nominees must possess "extensive" knowledge in two of three designated areas (cybersecurity, infrastructure security, and security risk management) and have five years' experience in fostering public-private partnerships in these areas. Additionally, the legislation established the statutory roles and responsibilities of sector risk management agencies (SRMAs) while mandating a Department of Homeland Security (DHS) review of the partnership structure and sector designations, among other provisions.

DHS submitted a report to Congress in November 2021, known as the "Section 9002(b) report." The report made several recommendations, including to clarify SRMA roles and responsibilities; review current sector structure and SRMA designations and establish a process for recurring assessments; update the NIPP and sector-specific plans; strengthen cross-sector coordination; establish consistent guidance for SRMA activities and resourcing; establish a National Infrastructure Assessment, Analysis, and Data Framework to improve infrastructure risk assessment practices; and consider more assertive use of federal authorities to augment voluntary public-private partnerships.

In addition, the DHS review contemplated creation of two new infrastructure sectors—Space and Bioeconomy—without formally recommending expansion of the current sector framework. In a letter to congressional leadership, President Biden endorsed the report recommendations and committed to providing updated policy guidance to facilitate implementation. In addition, he advocated for establishing mandatory minimum cybersecurity requirements across all sectors and expanding statutory authorities for infrastructure security and resilience. National Security Memorandum 22, issued in April 2024 as overarching federal critical infrastructure security and resilience policy guidance, largely reflected those priorities.

Sector Coordinating Councils

SCCs are the private-sector counterparts to GCCs. Joint meetings and other forms of collaboration between the two bodies have facilitated public-private partnerships. Each SCC has been made up of private-sector trade associations and individual critical infrastructure owner-operators.[109] They have had an advisory relationship with the federal government and also have coordination and information-sharing functions between government and private-sector stakeholders. In many cases, SCCs have also supported independently organized ISACs specific to their sector to facilitate information sharing among stakeholders. The National Council of ISACs listed 24 member organizations as of July 2025.[110] ISACs maintain operations centers, conduct preparedness exercises, and prepare a range of informational products for their members. Comprehensive data on the scale and scope of private-sector participation in SCC activities across critical infrastructure sectors is not available, but it varies widely depending on sector characteristics.[111]

[108] Jonathan Greig, "Noem Calls for Reauthorization of Cyberthreat Information Sharing Law During RSA Keynote," *The Record*, April 29, 2025, https://therecord.media/kristi-noem-rsa-keynote-info-sharing-law.

[109] According to the 2024 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 infrastructures are disrupted." See DHS, "Charter of the Critical Infrastructure Partnership Advisory Council," September 9, 2024, p. 6, https://www.cisa.gov/sites/default/files/2024-10/cipac-charter-2024-508.pdf.

[110] National Council of ISACs, "Home," https://www.nationalisacs.org/.

[111] A 2020 GAO report covered the adoption of the National Institute of Standards and Technology's cybersecurity framework across all sectors, which found that SRMAs did not have a consistent or systematic set of practices to (continued...)

SCCs are self-organized and self-governed private-sector organizations that may continue to operate in the absence of the CIPAC framework. However, they may modify previous information-sharing practices to account for the loss of confidentiality assurances provided by the CIPAC framework. Funding cutbacks and termination of certain programs and authorities may also affect SCC functions, which were customarily carried out in conjunction with GCC counterparts. For example, on March 6, 2025, the Trump Administration canceled funding for the Multi-State ISAC and Elections Infrastructure ISAC from congressionally appropriated funds for FY2025. The Multi-State ISAC provides a channel for sharing cyber threat information with SLTT governments. The Elections Infrastructure ISAC operates under its auspices. The canceled funds represented half of the Multi-State ISAC's operating budget for the remainder of the fiscal year.[112]

Cross-Sector Councils

Four cross-sector councils have represented key stakeholder groups whose broad interests are not specific to one sector. The State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) worked on infrastructure resilience partnerships among SLTT jurisdictions and represented their common governance-related interests in GCC and SCC deliberations.[113] The Critical Infrastructure Cross-Sector Council is the private-sector counterpart of the SLTTGCC, consisting of the chairs and vice chairs of the SCCs. It coordinates cross-sector issues among private-sector critical infrastructure stakeholders.

Other CIPAC Advisory Councils

In recent decades, a number of issue-area specific advisory bodies were established under CIPAC auspices to provide DHS with expert advice from nonfederal stakeholders on a confidential basis. The DHS termination of CIPAC included a number of these advisory bodies, including the Homeland Security Academic Partnership Council, Tribal Homeland Security Advisory Council, Artificial Intelligence Safety and Security Board, Public-Private Analytic Exchange Program, Homeland Security Science and Technology Advisory Committee, Cyber Investigations Advisory Board, and Data Privacy and Integrity Advisory Committee.[114]

FACA Advisory Councils

Some advisory councils were established outside the CIPAC framework and so have been subject to FACA transparency and disclosure requirements since then. The HSAC has provided advice and recommendations to the Secretary of Homeland Security on matters related to homeland security. Members were appointed by the Secretary and included leaders from state and local

---

determine framework adoption. See GAO, *Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements*, GAO-20-299, February 2020, https://www.gao.gov/assets/gao-20-299.pdf.

[112] See the "Impact of Funding Cuts to SLTTs" tab in Center for Internet Security, "MS-ISAC: Defending America's Critical Infrastructure," accessed September 10, 2025, https://www.cisecurity.org/ms-isac/defending-americas-critical-infrastructure.

[113] See CISA, "SLTTGCC Factsheet," 2021, https://www.cisa.gov/sites/default/files/2021-01/Factsheet_SLTTGCC.pdf. The most recent charter is from 2019, and the organization's DHS web page has been deleted. See "State, Local, Tribal, and Territorial Government Coordinating Council" in CISA, "CISA Tribal Affairs," https://www.cisa.gov/about/cisa-tribal-affairs.

[114] DHS, "Notice of Termination of Discretionary Federal Advisory Committees," 90 *Federal Register* 11995, March 13, 2025, https://www.federalregister.gov/documents/2025/03/13/2025-04011/notice-of-termination-of-discretionary-federal-advisory-committees.

government, first responder communities, the private sector, and academia. The Secretary also could establish subcommittees to focus attention on specific homeland security issues as needed. Critical-infrastructure-relevant subcommittees focused on cybersecurity and emerging technologies.

The National Infrastructure Advisory Council is constituted of senior industry leaders who advise the President and sector-specific agencies on critical infrastructure policy. It was not formally part of the NIPP partnership structure before its dissolution in 2025 but played an intermediary role among 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 E.O. 13231 of October 16, 2001, it was 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.[115]

Incentives for Private-Sector Participation

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 CIPAC partnership structure, government and private-sector representatives were expected to collaboratively ascertain what individual enterprise-level investments in security and resilience were necessary to manage critical infrastructure risk at the societal level.

While there is little question that businesses, government, and society have a "clear and shared interest" in CIR, it is often difficult at the policy level to work out exactly who should 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.[116]

By and large, the federal government relies on the private sector to voluntarily develop critical infrastructure 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."[117] 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.[118]

---

[115] E.O. 13231 of October 16, 2001, "Critical Infrastructure Protection in the Information Age," 66 *Federal Register* 53063, October 18, 2001, https://www.federalregister.gov/documents/2001/10/18/01-26509/critical-infrastructure-protection-in-the-information-age; and DHS, National Protection and Programs Directorate, National Infrastructure Advisory Council, *Charter*, December 11, 2017, p. 1, https://www.cisa.gov/sites/default/files/publications/niac-charter-dec2017-508.pdf.

[116] NIPP 2013, p. 1.

[117] NIPP 2013, p. 2. As of the date of this report, the 2013 NIPP is the current planning document for public-private partnerships for critical infrastructure risk management. The 2013 NIPP was due for replacement by April 2025 as required by NSM-22, but this timeline was subsequently superseded by the timeline in E.O. 14239.

[118] See James K. Hayes 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) (hereinafter Hayes and Ebinger, "Private Sector and Risk"); and Peter J. May and Chris Koski, "Addressing Public Risks: Extreme Events and Critical Infrastructures," *Review of Policy Research*, vol. 30, no. 2 (March 2013), pp. 139-159, https://doi.org/10.1111/ropr.12012 (hereinafter May and Koski, "Public Risks"). Hayes and Ebinger's statistical (continued...)

This pattern broadly applies internationally among developed countries (see **text box** below on "Public-Private Partnerships in Other Countries"). A 2019 report by the Organisation for Economic Co-operation and Development (OECD) found that voluntary information sharing and collaboration partnerships in advanced industrialized economies "[do not] necessarily guarantee a strong enough incentive structure to ensure that sufficient investments are effectively made to attain expected resilience targets."[119] Most developed countries augment voluntary policy instruments with regulatory mandates to spur investments in resilience in certain sectors.[120] Regulatory mandates tend to be favored for critical infrastructure sectors or subsectors 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.[121] According to an academic survey of public-private partnerships for critical infrastructure security, collaborative approaches more broadly apply "as risks become more privatized" and "harms are more divisible and isolated with respect to their impacts."[122]

Public-Private Partnerships in Other Countries

The Organisation for Economic Co-operation 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' critical infrastructure policy frameworks were relatively immature and that all faced significant challenges. Critical infrastructure owner-operators might be reluctant to share information "if they fear [doing so] 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.[123]

There are three main incentives for industry participation: 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 officials in a nonregulatory setting.[124]

Congress acted to reduce barriers to information sharing between the public and private sectors through the Critical Infrastructure Information Act of 2002 (P.L. 107-296, Subtitle B), which is designed to ensure confidentiality of industry information on vulnerabilities or security incidents shared with DHS in good faith under the Protected Critical Infrastructure Information (PCII) program.[125] Likewise, a number of public-private coordination councils established under the authority of presidential directives provide a forum for policy discussions and deliberation.

study suggests that social altruism plays a role in private-sector investment decisions but that financial cost-benefit calculations predominate among respondents in a survey. May and Koski highlight cognitive, behavioral, and organizational barriers to collaboration and investment.

[119] OECD Risk Management Review, p. 56.

[120] OECD Risk Management Review, p. 84.

[121] See Peter W. Huber, "The Bhopalization of U.S. Tort Law," *Issues in Science and Technology*, vol. 2, no. 1 (Fall 1985), pp. 73-82; and David Demeritt et al., "Mobilizing Risk: Explaining Policy Transfer in Food and Occupational Safety Regulation in the UK," *Environment and Planning A*, vol. 47, no. 2 (February 2015), pp. 373-391.

[122] May and Koski, "Public Risks," p. 156.

[123] OECD Risk Management Review, p. 52.

[124] NIPP 2013, pp. 1-2.

[125] P.L. 107-296, §222. The Protected Critical Infrastructure Information (PCII) program contains protections against disclosure of sensitive critical infrastructure 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.

In 2015, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA 2015; P.L. 114-113, Title I), which provided liability and certain law enforcement exemptions to the private sector to facilitate bilateral cyber threat information sharing between private and public sector entities. This law also required the Director of National Intelligence and the Departments of Homeland Security, Defense, and Justice to develop procedures to share cybersecurity threat information with private entities; nonfederal government agencies; state, tribal, and local governments; the public; and entities under threats. The authorizations within CISA 2015 expired at the end of September 2025 but were temporarily reauthorized under a continuing resolution in November of that year. They were subsequently authorized for all of FY2026 as part of the Consolidated Appropriations Act, 2026 (P.L. 119-75).[126]

Several Members of the 119th Congress have introduced bills for a long-term reauthorization of CISA 2015. The Widespread Information Management for the Welfare of Infrastructure and Government Act (WIMWIG; H.R. 5079) would extend CISA 2015 until 2035. Additionally, it would make several amendments to the law, adding definitions of *critical infrastructure* (citing the CIPA definition) and *artificial intelligence*, as well as additional sharing and updating requirements, among other provisions.[127] S. 1337 would extend CISA 2015 until 2035 with no other changes. In October 2025, efforts to pass the bill by unanimous consent on the Senate floor were unsuccessful.[128]

The Relationship Between Voluntary Partnerships and Federal Regulation

Initial federal efforts to establish a national CISR enterprise generally emphasized voluntary public-private partnerships, rather than regulation, as the primary mechanism for meeting security and resilience goals. 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."[129] The Homeland Security Act created an organization—DHS—with wide-ranging responsibilities but relatively narrow regulatory mandates. However, perceived risk management failures in the private sector that highlighted growing cyber-related threats to critical infrastructure have led successive Administrations and Congresses to assert more authority over critical infrastructure to ensure compliance with federal risk management goals.

For example, Congress granted the Transportation Security Administration (TSA), a DHS agency, authorities to regulate pipeline operators under the Homeland Security Act. However, TSA did not exercise these authorities for many years, favoring nonregulatory collaboration with pipeline operators to develop and encourage adoption of voluntary consensus standards for pipeline cybersecurity.[130] However, TSA issued binding directives to pipeline operators after a 2021

[126] For more information, see CRS In Focus IF12959, *The Cybersecurity Information Sharing Act of 2015: Expiring Provisions*, by Chris Jaikaran.

[127] See Alex Snyder, "H.R. 5079 (119): House Approves Crucial Cyber Threat Reauthorization Bill Ahead of Sept. 30 Deadline, While Senate Stalls," *PoliticoPro*, September 17, 2025, https://legislation.politicopro.com/bill/US_119_HR_5079/pro-bill-analysis/00000199-3f8d-dd64-a19b-3fffa4c20001.

[128] "Actions for S. 1337," *PoliticoPro*, October 7, 2025, https://legislation.politicopro.com/bill/US_119_S_1337?activeTabs=actions.

[129] PDD-63, p. 3.

[130] CRS Report R44939, *Cybersecurity for Energy Delivery Systems: DOE Programs*, by Paul W. Parfomak, Chris Jaikaran, and Richard J. Campbell. The authors find that the Transportation Security Administration (TSA) relies on "voluntary industry compliance with the agency's security guidance and best practice recommendations," despite regulatory and inspection authorities granted to the agency under the Implementing Recommendations of the 9/11 Commission Act of 2007.

ransomware attack against the Colonial Pipeline Company that disrupted retail gasoline supplies on the East Coast for nearly a week. TSA required covered operators to report cybersecurity incidents, designate a Cybersecurity Coordinator to coordinate with federal agencies, and report results of risk assessments to TSA and CISA.[131]

In general, 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 therefore are treated as industrial safety and reliability issues in most cases.[132] 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.[133]

Agencies with dual responsibilities for regulation and partnership typically separate the two roles. However, private-sector participation in voluntary CISR programs and activities is often conditioned by the structure of federal regulatory authorities and oversight. For example, in the Energy critical infrastructure sector, oil and gas industry organizations have been most active in developing critical infrastructure risk management standards and investing in voluntary public-private partnerships in heavily regulated industry segments, such as offshore fuel exploration and extraction. By contrast, the less-regulated onshore segment does not appear to have produced comparable public-private partnerships or publicly available safety and security data.[134]

Conversely, voluntary partnership programs may contribute to development of regulatory programs. For example, public-private coordination bodies in each of the 16 designated critical infrastructure sectors developed sector-specific critical infrastructure risk management plans under the voluntary NIPP framework. Nearly a decade later, CISA used these plans to evaluate the applicability of the proposed CIRCIA program rules to critical infrastructure entities. The agency's explanation of its proposed rule stated that it "considered the variety of entities described in the sector profiles in the [sector-specific plans] when determining the scope of the Applicability section."[135]

Assessing the Effectiveness of Voluntary Partnerships

The underlying policy premise of the coordinating bodies established under the 2013 NIPP and CIPAC was that removing or mitigating disincentives to information sharing and increasing trust

[131] TSA Security Directive Pipeline-2021-01114 under 49 C.F.R. Part 114.

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

[133] DHS, *Nuclear Reactors, Materials, and Waste Sector-Specific Plan: An Annex to the NIPP 2013*, 2015, p. 2, https://climateandsecurity.org/wp-content/uploads/2025/01/dhs-nipp-ssp-nuclear-2015-508.pdf. DHS maintains a support component named the Office for Countering Weapons of Mass Destruction (CWMD) to coordinate multi-jurisdictional efforts to detect or interdict illicit radiological materials. CWMD's FY2026 budget justification proposed dissolving the office and redistributing personnel and funding to other DHS components "to create synergies and efficiencies in accomplishing the mission previously performed by the Office of Countering Weapons of Mass Destruction Office (CWMD)." See DHS, *Countering Weapons of Mass Destruction Budget Overview: Fiscal Year 2026 Congressional Justification*, June 25, 2026, p. 5, https://www.dhs.gov/sites/default/files/2025-06/25_0613_cwmd_fy26-congressional-budget-justificatin.pdf.

[134] For more information, see the "Discussion and Analysis" section in CRS Report R46987, *Critical Infrastructure Risk Management: Securing the Oil and Gas Supply Chain*, by Brian E. Humphreys.

[135] CIRCIA proposed rule on reporting requirements, p. 23677, https://www.federalregister.gov/d/2024-06526/page-23677.

between the public and private sectors would lead to greater industry willingness to invest in system-level resilience. This prompts two questions:

- To what extent have private sector owner-operators actually embraced collaboration and information-sharing initiatives offered by federal departments and agencies under the current partnership system?
- Has private-sector participation in these initiatives incentivized effective investments (beyond those made for business reasons) in programs to reduce overall *public* risk?

Given the diversity and breadth of the critical infrastructure enterprise as currently defined, the answers to these questions have varied across (and sometimes within) sectors and various subsectors. Rigorous empirical analyses that might systematically shed light on the extent and effectiveness of public-private partnerships under the NIPP framework are scarce. Anecdotal reports indicate that at least some partnership programs have garnered significant stakeholder commitment.

For example, in February 2025, the National Association of Secretaries of State highlighted benefits of CISA partnership with state and local elections authorities through Election Infrastructure subsector coordinating bodies in response to a DHS review of CISA election security activities. Addressing the Secretary of Homeland Security, the letter praised CISA for providing cybersecurity services to election offices, physical security assessments of polling places, support for cyber threat reporting and analysis through the Elections Infrastructure ISAC, incident response support, classified and unclassified briefings, and the forum provided by the subsector's GCC.[136]

Additionally, some private-sector stakeholders have created new ISACs independently and, in some cases, advocated for federal designation of new infrastructure sectors. For example, the Food and Agriculture sector's ISAC was originally formed in 2002 but closed in 2008 after failing to attract an active user base.[137] Sector stakeholder interests were then represented by the Food and Ag Special Interest Group (Food and Ag SIG) within the IT ISAC. Some observers criticized this arrangement as inadequate to the scale of cyber threats faced by the Food and Agricultural sector.[138] Industry leaders rebranded the Food and Ag SIG as the Food and Agriculture sector ISAC in 2023.[139] Although the new ISAC continued to operate under IT ISAC

[136] Letter from Steve Simon, National Association of Secretaries of State (NASS) President and Minnesota Secretary of State, and Michael Watson, NASS President-Elect and Mississippi Secretary of State, to Kristi Noem, Secretary of Homeland Security, February 21, 2025, https://www.nass.org/sites/default/files/Election Cybersecurity/2.21.25 NASS Board Letter to Sec. Noem.pdf. For more information on the development of the Election Infrastructure critical infrastructure sector, see CRS In Focus IF11445, *The Election Infrastructure Subsector: Development and Challenges*, by Brian E. Humphreys and Karen L. Shanton.

[137] The Food Marketing Institute, an industry group, established an agriculture Information Sharing and Analysis Center (ISAC) in 2002 prior to the establishment of DHS as an agency but disbanded it in 2008 due to "lack of activity and information flow," according to media reports. See "Food Sector Abandons Its ISAC," *Security Management*, September 1, 2008, https://www.asisonline.org/security-management-magazine/articles/2008/09/food-sector-abandons-its-isac/.

[138] See Eric Geller, "The Dangerous Weak Link in the U.S. Food Chain," *Wired*, April 6, 2023, https://www.wired.com/story/us-food-agriculture-isac-cybersecurity/. The Food and Agriculture Industry Cybersecurity Support Act, introduced in the 118th Congress (S. 2393/H.R. 1219), would have mandated creation of a cybersecurity clearinghouse for the sector hosted by the National Telecommunications and Information Administration, a Department of Commerce agency.

[139] Food and Ag-ISAC, "Built By Industry for Industry," https://www.foodandag-isac.org/, and "Food and Ag-ISAC Forms to Protect Agrifood Sector from Cybersecurity Threats," *Food Safety Magazine*, May 26, 2023, (continued...)

auspices, its leaders asserted that the change would raise the profile of the organization and clarify its mission.[140]

In 2019, industry stakeholders in space and related technologies founded Space ISAC.[141] Some stakeholders have advocated for designation of space systems, services, and technology as a critical infrastructure sector. Bills for this purpose were introduced in the 117th and 118th Congresses.[142]

However, other evidence of effectiveness and stakeholder commitment has generally been more mixed. A 2013 study found that fewer than half of the 16 critical infrastructure sectors had strong "communities of interest" that actively engaged in CIP issues through NIPP partnership structures. Critical infrastructure 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.[143] A 2011 study found that the most important factor in private-sector risk mitigation investment was a company's own cost-benefit analysis and that many critical infrastructure owner-operators believed that government would (or should) cover externalized social costs incurred by loss or disruption of company facilities due to a terrorist attack.[144]

GAO testimony provided to Congress in 2014 asserted that DHS partnership efforts faced challenges, and identified three key factors that impacted effectiveness of the partnership approach: "(1) recognizing and addressing barriers to sharing information, (2) sharing results of DHS assessments with industry and other stakeholders, and (3) measuring and evaluating the performance of DHS partnerships."[145]

GAO found that DHS did not systematically collect data on reasons for industry participation or nonparticipation in security surveys and vulnerability surveys, and whether or not security improvements were made as a result.[146] GAO asserted that DHS could not adequately evaluate program effectiveness absent these measures. Overall, the picture that emerges from this testimony and other sources is one of extensive partnership activity across multiple critical infrastructure sectors but relatively few measures to systematically assess the effectiveness of this activity in meeting CIR goals.[147]

In a 2023 report on SRMAs' implementation of FY2021 NDAA statutory responsibilities, GAO found continuing challenges. SRMA officials asserted that the "voluntary nature of private sector participation" and "limited or no dedicated resources for SRMA duties" made it difficult to gain

---

https://www.food-safety.com/articles/8617-food-and-ag-isac-forms-to-protect-agrifood-sector-from-cybersecurity-threats.

[140] Tim Starks, "The Food and Agriculture Industry Gets a New Center to Share Cybersecurity Information," *Washington Post*, May 24, 2023, https://www.washingtonpost.com/politics/2023/05/24/food-agriculture-industry-gets-new-center-share-cybersecurity-information/.

[141] Space ISAC, "About Us," https://spaceisac.org/about-us/.

[142] H.R. 3713 and H.R. 5017.

[143] May and Koski, "Public Risks," pp. 151-153.

[144] Hayes and Ebinger, "Private Sector and Risk."

[145] GAO, *Critical Infrastructure Protection: Observations on Key Factors in DHS's Implementation of Its Partnership Approach*, GAO-14-464T, March 26, 2014, p. 2, https://www.gao.gov/assets/gao-14-464t.pdf (hereinafter GAO-14-464T).

[146] GAO-14-464T, p. 15.

[147] In 2018, DHS indicated that it would survey industry partners in the electricity subsector to ascertain what correlations—if any—existed among industry awareness of risks posed by electromagnetic hazards, exposure to DHS information-sharing initiatives, and investment in mitigation measures. DHS, *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.

visibility on sector security issues and provide effective risk assessments.[148] Further, GAO found that only one SRMA—the Environmental Protection Agency—had instituted procedures to "track and assess the effectiveness of their efforts."[149]

Potential Revisions to the All-Hazards Approach and Increased Role of States in Risk Management

On March 18, 2020, President Trump signed E.O. 14239, "Achieving Efficiency Through State and Local Preparedness," which, according to the Administration's accompanying fact sheet, requires "a review of all infrastructure, continuity, and preparedness policies to modernize and simplify federal approaches."[150] E.O. 14239 directs the Assistant to the President for National Security Affairs—or National Security Advisor—to complete a review of NSM-22 and certain other related directives within 180 days and to "recommend to the President the revisions, recissions, and replacements necessary to achieve a more resilient posture."[151]

E.O. 14239 states that "it is the policy of the United States that State and local governments and individuals play a more active and significant role in national resilience and preparedness." It does not detail specific agency taskings that would accomplish this goal, instead directing the National Security Advisor to revise existing policy guidance based on a new National Resilience Strategy that would replace the document published during the waning days of the Biden Administration in January 2025. The new strategy has not been released as of February 2026.

In addition to its broad decentralization mandate, the directive mandates a shift from an "all-hazards approach" to a "risk-informed approach" based on a review of NSM-22 and other existing guidance by the National Security Advisor. E.O. 14239 does not provide detailed explanation of how these approaches differ from one another. All-hazards approaches often incorporate assessments of event likelihood, asset vulnerability, and consequence of loss or disruption to prioritize risk mitigation policy and investments. According to the White House fact sheet on E.O. 14239, risk-informed approaches prioritize "resilience and action over mere information sharing."[152]

Previous White House and agency guidance over several Administrations emphasized information sharing as a core element of the CISR enterprise. E.O. 14239 tasks the National Security Advisor with developing detailed revisions of existing CISR guidance and providing detailed new guidance to support implementation of a new National Resilience Strategy. The strategy was due to be completed by June 17, 2025. This latter document would supersede the National Resilience Strategy published by the Biden Administration in January 2025.

As of February 2026, CRS was unable to find a publicly available copy of the strategy or any record of its completion. The National Security Advisor's recommendations of rescissions or

[148] GAO, *Critical Infrastructure Protection: Time Frames to Complete DHS Efforts Would Help Sector Risk Management Agencies Implement Statutory Responsibilities*, GAO-23-105806, February 2023, p. 20, https://www.gao.gov/assets/d23105806.pdf (hereinafter GAO-23-105806).

[149] GAO-23-105806, p. 26. This is the first of a series of reports on SRMA effectiveness. The FY2021 NDAA required the Comptroller General to submit a report on this topic within two years of enactment and then every 4 years thereafter for 12 years.

[150] White House, "Fact Sheet: President Donald J. Trump Achieves Efficiency Through State and Local Preparedness," March 18, 2025, https://www.whitehouse.gov/fact-sheets/2025/03/fact-sheet-president-donald-j-trump-achieves-efficiency-through-state-and-local-preparedness/ (hereinafter White House 2025 Preparedness Fact Sheet).

[151] E.O. 14239 of March 18, 2025.

[152] White House 2025 Preparedness Fact Sheet.

modifications of NSM-22 and certain other policy documents to align with the new strategy were due by September 14, 2025 (see "National Security Memorandum 22" section). As of February 2026, it is unknown whether this strategy has been provided. In addition, E.O. 14239 directed the National Security Advisor to produce a national risk register by December 13, 2025, which would "inform the Intelligence Community, private sector investments, State investments, and Federal budget priorities." As of February 2026, CRS was unable to locate a publicly available register.

Stakeholder Perspectives on E.O. 14239

Stakeholder perspectives on E.O. 14239 focused on potential fiscal and operational consequences of reforms outlined in the document. For example, E.O. 14239 might create additional demands on state and local government budgets. Some stakeholders expressed concern that E.O. 14239 might require greater operational reliance on private-sector entities for infrastructure security services, streamlining of infrastructure resilience investments to mitigate high-priority risks, and acceptance of more risk in other lower priority areas.[153] According to one international advisory firm, E.O. 14239 "fundamentally shifts responsibility for resilience and risk management from the federal government to state and local governments. Any gaps left by state and local authorities will necessarily be absorbed by property owners, residents, businesses and their insurance carriers."[154]

Some parties noted that E.O. 14239 provided broad outlines of policy change but that a fuller assessment of potential costs and benefits could not be made until risk and strategy guidance necessary for full implementation was complete and publicly available.[155] Although observers noted budgetary and resource concerns, some also expressed optimism that reforms might encourage municipalities to take greater local responsibility for infrastructure security and provide opportunities for regional collaboration.[156]

Proposed CISA FY2026 Budget

The CISA FY2026 budget justification contained cutbacks that aligned with the broad policy preferences set forth in E.O. 14239—that is, reduction of federal investment in CISR programs and activities in favor of state and local investments. The CISA FY2026 budget justification requested an overall appropriation of $2.38 billion—a 19% decrease from the FY2025 enacted appropriation of $2.87 billion.[157] The budget request includes a reduction from 3,294 to 2,324 full-time employees—a 30% decrease.[158] Cuts in the proposed FY2026 budget focus on CISA support for public-private partnerships for CISR, risk assessments, cybersecurity, and provision of agency expertise and services through regional operations. **Table 2** summarizes changes to CISR-related program areas in the Operations and Support category of the proposed FY2026 budget.

---

[153] Victoria Salinas et al., "All Resilience Is Local: Implications of Federal Devolution of Disaster Preparedness & Response," Teneo, May 6, 2025, https://www.teneo.com/insights/articles/all-resilience-is-local-implications-of-federal-devolution-of-disaster-preparedness-response/ (hereinafter "All Resilience Is Local").

[154] "All Resilience Is Local."

[155] National League of Cities, "Achieving Efficiency Through State and Local Preparedness," March 19, 2025, https://www.nlc.org/wp-content/uploads/2025/10/Achieving-Efficiency-Through-State-and-Local-Preparedness-EO-Fact-Sheet.pdf.

[156] Mindy L. Zoghlin, "What Does the 'Achieving Efficiency Through State and Local Preparedness' EO Mean for NYS Municipalities?," Underberg & Kessler LLP, April 3, 2025, https://www.underbergkessler.com/post/what-does-the-achieving-efficiency-through-state-and-local-preparedness-eo-mean-for-nys-municipali.

[157] CISA FY2026 budget justification, p. 7.

[158] CISA FY2026 budget justification, p. 8.

Table 2. CISA FY2026 Budget Justification

Summary of Requested Appropriations for Operations and Support in Thousands of Dollars

Program Area	Major Activities	FY2025 Budget (Enacted)	FY2026 Budget (Requested)	FY2025-FY2026 Change
Cybersecurity	Prevent cyberattacks on FCEB systems and critical infrastructure networks, reduce vulnerabilities, and respond to incidents.	$1,181,648	$965,553	($216,095)
Infrastructure Security	Lead and coordinate national programs and policies for CISR. Provide technical expertise to stakeholders, conduct and facilitate risk assessments, and provide information on emerging threats and hazards such as nation-state threats to critical infrastructure.	$159,129	$302,946[a]	$143,817
Integrated Operations	Support CISA's role as National Coordinator for CISR by disseminating risk and threat information, providing intelligence context to support key decisionmaking, and delivering CISA programs and services through 10 regional offices to support stakeholders.	$228,378	$182,139	($46,239)
Risk Management Operations	Support the NRMC, which partners with and supports SRMAs in their efforts to analyze, understand, and reduce risks to the nation's critical infrastructure using cross-sector and strategic risk analyses.	$133,870	$36,406	($97,464)
Stakeholder Engagements and Requirements	Support CISA's roles, responsibilities, and functions as the SRMA for 8 of the nation's 16 critical infrastructure sectors on behalf of DHS and as the National Coordinator to all 16 sectors.	$99,718	$37,519	($62,199)

Source: CRS, adapted from Department of Homeland Security (DHS), *Cybersecurity and Infrastructure Security Agency Budget Overview: Fiscal Year 2026 Congressional Justification*, June 9, 2025, p. 7, https://www.dhs.gov/sites/default/files/2025-06/25_0613_cisa_fy26-congressional-budget-justificatin.pdf.

Notes: CISR = critical infrastructure security and resilience; FCEB = Federal Civilian Executive Branch; NRMC = National Risk Management Center; SRMA = sector risk management agency. Dollar amounts in parentheses signify proposed reduction from enacted FY2025 appropriation. According to the Cybersecurity and Infrastructure Security Agency (CISA), "the Operations and Support (O&S) appropriation funds the core operations of CISA to enhance the security and resilience of critical infrastructure against terrorist attacks, cyber events, and other security incidents" (p. O&S – 5).

a. Includes a transfer of $237.8 million from the Countering Weapons of Mass Destruction Office, which would be discontinued under the proposed budget.

The CISA Procurement, Construction, and Improvements appropriation request would also decrease funding for cybersecurity and infrastructure security programs if enacted. For example, the CyberSentry program, which provides "cross-sector, real-time identification of malicious threats to IT and Operational Technology (OT)/Industrial Control Systems (ICS) networks on participating partner networks," would receive $5 million for FY2026—$15 million less than the previous year.[159] According to 2023 CISA congressional testimony, the National Cybersecurity Protection System provides a technological foundation that enables CISA to secure and defend

[159] CISA FY2026 budget justification, p. PC&I – 20.

FCEB agencies' IT infrastructure against advanced cyber threats.[160] The program received $30 million in FY2025. The FY2026 request would eliminate funding.[161] Funding for the Cyber Analytics and Data System, which—according to CISA—"supports the procurement and sustainment of unclassified cyber mission infrastructure, operations tools, and mission engineering capabilities that enable the integration and analysis of data, collaboration, and knowledge management functions that strengthen the cybersecurity posture of supported partners and stakeholders," would be reduced from $145.5 million in FY2025 to $65.8 million in FY2026.[162]

Congressional Appropriations for FY2026

As of the date of this report, the FY2026 appropriations for DHS are under congressional debate.[163] The 119th Congress passed a continuing appropriations resolution, enacted on November 12, 2025, known as the Continuing Appropriations, Agriculture, Legislative Branch, Military Construction and Veterans Affairs, and Extensions Act, 2026 (P.L. 119-37), which extended FY2025 funding levels for CISA until January 30, 2026, when DHS appropriations lapsed.

Congressional appropriators have introduced homeland security spending bills, but full-year appropriations for CISA for FY2026 have not been enacted as of the date of this report.[164] Congressional priorities regarding certain CISR policies, programs, and activities were identified in the appropriations committee reports. The House report recommended a $2.7 billion appropriation for CISA—a $360 million increase over the requested level but a $135 million decrease from the FY2025 appropriation. The Senate report recommended appropriations of nearly $2.9 billion for CISA. Notably, the Senate report—unlike the House report—includes recommended spending to support Election Security Advisors and continuation of the Elections Infrastructure ISAC.[165] Additional language in the Senate report directs the executive branch to maintain personnel strength necessary to perform statutory missions and staff field offices.[166] On March 5, 2026, the House passed a DHS appropriations bill (H.R. 7744) that would provide $2.6 billion for CISA. Senate action on the bill was still pending as of the date of this report.

Other Legislation

Some grant programs, such as the Cybersecurity Grant Program (administered by CISA), may fund state-level CIP or CIR initiatives related to cybersecurity. In November 2025, the House passed the Protecting Information by Local Leaders for Agency Resilience Act (PILLAR Act; H.R. 5078), which would extend the State and Local Cybersecurity Grant Program through

[160] U.S. Congress, House Committee on Homeland Security, Subcommittee on Cybersecurity and Infrastructure Protection, *CISA 2025: The State of American Cybersecurity from CISA's Perspective*, hearing, 118th Cong., 1st sess., April 27, 2023, H.Hrg. 118-9, p. 10.

[161] CISA FY2026 budget justification, p. PC&I – 10.

[162] CISA FY2026 budget justification, pp. PC&I – 7-8, PC&I – 11.

[163] Jordain Carney, "Shutdown Talks Make Little Progress as DHS Bill Stalls in Senate," *E&E News*, February 25, 2026, https://www.eenews.net/articles/shutdown-talks-make-little-progress-as-dhs-bill-stalls-in-senate/.

[164] See H.R. 4213 and H.R. 7147.

[165] U.S. Congress, Senate Committee on Appropriations, *Explanatory Statement for the Homeland Security Appropriations Bill, 2026*, 119th Cong., 2nd sess., p. 90, https://www.appropriations.senate.gov/imo/media/doc/fy26_homeland_security_report.pdf (hereinafter *Explanatory Statement for the Homeland Security Appropriations Bill, 2026*).

[166] *Explanatory Statement for the Homeland Security Appropriations Bill, 2026*, p. 98.

FY2035, expand the scope of the program, and impose certain limits on the use of grant funds. It would expand the scope of systems that may be secured using grant funds to include operational technology systems and specifies that systems using artificial intelligence are included. Such systems must be maintained, owned, or operated by or on behalf of state, local, or tribal governments. The State and Local Cybersecurity Grant Program Reauthorization Act (S. 3251), introduced in the Senate, would extend the program through FY2026.

Policy Options and Considerations for Congress

For the past several decades, the national CISR enterprise has been largely defined by federal investment in private-public partnerships across designated critical infrastructure sectors. These partnerships are guided by governmental and private-sector coordination bodies that were created to facilitate exchange of policy ideas and best practices, development and communication of national priorities, and exchange of information and technical assistance on threats and hazards. In 2025, the Trump Administration issued directives and budget proposals that may reduce federal support and involvement in public-private partnerships and reduce the scale and scope of federal cybersecurity and infrastructure security services provided to critical infrastructure owner-operators, as well as state and local governments (see "Public-Private Partnership Coordination Bodies" and "Potential Revisions to the All-Hazards Approach and Increased Role of States in Risk Management" sections).

Shift Responsibility to State and Local Governments

Congress may choose to legislatively ratify the Administration's intent to shift core CISR governance functions—and responsibility for funding them—to the states, as outlined in E.O. 14239. Congress may decide through appropriations and other actions to unwind or curtail CISR public-private partnerships and devolve related roles and responsibilities to the states, aligning legislative policy with Administration priorities set forth in E.O. 14239. Significant decreases in federal presence and support might create more localized CISR risk management enterprises in place of the more centralized enterprise promoted by the federal government between the late 1990s and the beginning of the second Trump Administration.

This might incentivize SLTT authorities to take increased responsibility for ensuring resilience of critical infrastructure functions in their jurisdictions by investing more in local capabilities, finding efficiencies, and innovating new approaches that can be sustained without federal support. A multiplicity of different standards and approaches for infrastructure security and resilience partnerships may lead to the creation of one or more successful models that could be adopted on a wider basis.

However, localized risk management might have drawbacks as well. The CISR risk management discipline has traditionally relied on information sharing and analysis that generally became more effective with increasing scale and centralization. Therefore, localizing CISR risk management might lead to diminished overall effectiveness if the national CISR enterprise became more compartmentalized and shared understandings of infrastructure risks diminished among stakeholders. Further, SLTT authorities might have to duplicate functions currently performed by federal entities and might not be able to supply adequate resources for such functions.

Considerations for Federal and State Collaboration

In recent decades, many SLTT capabilities were created and defined in relation to federal coordination and leadership of a national CISR enterprise. CISA and other federal agencies

provide intelligence and analysis, policy coordination frameworks, and technical support, among other services, which enable various SLTT infrastructure security and resilience programs and activities. Conversely, federal agencies rely on SLTT counterparts to implement national-level initiatives at the local level. Therefore, SLTT and federal capabilities have been highly interdependent.

Options for Congress include maintaining or expanding this federated structure by continuing to authorize and fund programs that support SLTT capabilities at the federal, state, and local levels. For example, Congress could support reauthorization of the State and Local Cybersecurity Grant Program, as proposed in H.R. 5078, to assist states in expanding their cybersecurity capabilities. It could also provide resources to help more states conduct technical analyses of critical infrastructure to support nominations to the NCIPP or other purposes. Congress may restore federal support for partnership resources, such as the Multi-State ISAC and regional offices that support CISA's security advisor and other programs intended to enable SLTT capabilities.

Legislation may be introduced to reestablish a legal framework for public-private partnerships previously established under (now-terminated) CIPAC auspices, to include provisions for confidential discussions and sharing of sensitive infrastructure information. A longer reauthorization of CISA 2015—due to sunset on September 30, 2026—would facilitate bilateral information sharing (see "Incentives for Private-Sector Participation" section). Congress may also exercise oversight over implementation of the forthcoming ANCHOR partnership framework that would replace CIPAC for multilateral information sharing, according to media reports.[167] It may also consider appropriations to fund public-private partnerships led or coordinated by CISA.

Further, Congress may continue to exercise oversight over CISA implementation of CIRCIA and consider funding levels both for development and implementation of regulations and for analysis and dissemination of risk information to critical infrastructure partners. CIRCIA is a core element of the previously established partnership model, which has relied heavily on private-sector sharing of cyber threat information to function. If fully implemented, CIRCIA would potentially reinforce this model through regulations that require covered critical infrastructure entities to report certain cyber incidents to CISA. The DHS FY2026 budget request proposed largely maintaining funding for CIRCIA but reducing or eliminating various CISA capabilities to analyze the incident data it receives from covered entities and share relevant risk information with critical infrastructure stakeholders (see "Cyber Incident Reporting for Critical Infrastructure Act of 2022 and Identification of Critical Infrastructure Entities" section).

Other Policy Considerations

In addition to appropriations legislation, Congress may also choose what—if any—oversight to exercise over executive branch administration of programs it authorizes and funds, especially in domains such as election infrastructure security, technical assistance to states and critical infrastructure operators, and cyber information sharing—programs that the Trump Administration has sought to eliminate or reduce unilaterally. Possible oversight issues include staffing levels for technical assistance programs, allocation of funds to the Elections Infrastructure ISAC, completion of CIRCIA rulemaking and implementation of related regulatory and analytical activities, effectiveness of existing public-private partnerships, and establishment or

[167] Derek B. Johnson, "Sources: DHS Finalizing Replacement for Disbanded Critical Infrastructure Security Council," *CyberScoop*, January 14, 2026, https://cyberscoop.com/dhs-anchor-cipac-replacement-critical-infrastructure-cybersecurity-liability-protections/.

reestablishment of institutional frameworks for public-private coordination and information sharing.

Additionally, the National Resilience Strategy and other policy documents mandated under E.O. 14239, which are necessary for its full implementation, have not been completed or made public as of the date of this report. Congress may seek clarification from the Administration on timelines for production of detailed policy documents that would provide greater clarity and transparency for oversight purposes and inform efforts of stakeholders in SLTT jurisdictions to adapt to changes. Further, Congress may seek to work with the Administration to facilitate confirmation of a permanent CISA Director in order to clarify lines of authority and accountability. Alternately, Congress may choose not to exercise its authorities in these areas. Forgoing the use of these authorities would likely create space for greater executive branch discretion in shaping the CISR enterprise free from the constraints of any explicit policy framework.

Appendix A. Glossary of Key Terms

Table A-1 shows definitions for key critical infrastructure terminology used in this report.

Table A-1. Glossary of Key Terms

Term	Definition
Critical Infrastructure	Machinery, facilities, and information that enable vital functions of governance, public health, and the economy. Defined in statute 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."[a]
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 critical infrastructure risk management and administration of public-private partnership system established by PPD-21 and NIPP 2013, and reaffirmed by NSM-22.
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.[b]
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 DHS. Subsequent critical-infrastructure-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 critical infrastructure 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 agencies and other stakeholders and vetted by DHS according to consequence-based criteria of fatalities, economic loss, mass evacuation length, and national security impacts.
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 established the NRMC to manage national critical infrastructure risk in partnership with federal, SLTT, and private-sector stakeholders.
National Security Memorandum 22 (NSM-22)	Presidential directive issued in April 2024 that superseded PPD-21. NSM-22 envisioned an accelerated risk management cycle for the critical infrastructure security and resilience enterprise, requiring biennial updates of national infrastructure risk management plans from designated officials and agencies, as well as enhanced intelligence collection, analysis, and sharing. Additionally, it mandated a more assertive use of federal authorities to encourage private-sector compliance with minimum resilience standards. Executive Order 14239 of March 18, 2025, directed the National Security Advisor to review—and if necessary modify—NSM-22.
Operational Components of DHS	Component agencies of DHS with operational mission responsibilities. These are CISA, 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 the first high-level policy guidance for CIP in the contemporary era.
Presidential Policy Directive 21 (PPD-21)	Policy guidance released by the Obama Administration in 2013 for critical infrastructure security, superseding HSPD-7. Maintained much of the previous policy framework of HSPD-7 but placed greater emphasis on all-hazards resilience and highly distributed public-private partnerships. Superseded by NSM-22.
Protected Critical Infrastructure Information (PCII)	DHS program established under provisions of the Critical Infrastructure Information Act of 2002, which ensures confidentiality of certain industry critical infrastructure 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 SRMAs and related GCCs on the entire range of critical infrastructure security and resilience policies and efforts for a given critical infrastructure sector.
Sector-Specific Agency (SSA)	Federal government agency with knowledge and responsibilities specific to a given critical infrastructure sector assigned primary responsibility for implementation of PPD-21 in that sector.
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct	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,

Terrorism Act of 2001 (USA PATRIOT Act)	national public health or safety, or any combination of those matters." This definition has been widely adopted in other laws and policy documents.

Source: CRS and sources noted below.

Notes: DOD = Department of Defense; DHS = Department of Homeland Security; SLTT = state, local, tribal, and territorial.

a. 42 U.S.C. §5195c(e).

b. DHS, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 2013, p. 12, https://www.nist.gov/system/files/documents/cybercommission/-DHS-_National_Infrastructure_Protection_Plan_-NIPP.pdf.

Appendix B. National Critical Functions

In 2019, the Cybersecurity and Infrastructure Security Agency (CISA) promulgated the National Critical Function (NCF) set to improve methods for infrastructure risk assessment and enable better collaboration across multiple critical infrastructure sectors. CISA defines NCFs as "the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[168] **Table B-1** shows the four categories of the NCF set and lists the functions under each category.

Table B-1. National Critical Function Set

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

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

Connect	Distribute	Manage	Supply
		Provide Capital Markets and Investment Activities	
		Provide Consumer and Commercial Banking Services	
		Provide Funding and Liquidity Services	
		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: Cybersecurity and Infrastructure Security Agency (CISA), "National Critical Functions Set," https://www.dhs.gov/cisa/national-critical-functions-set.

Appendix C. Sector and Cross-Sector Coordinating Structures

Figure C-1 shows coordinating structures for public-private critical infrastructure security and resilience (CISR) partnerships.

Figure C-1. Sector and Cross-Sector Coordinating Structures

		Critical Infrastructure Partnership Advisory Council		
Critical Infrastructure Sector	**Sector Specific Agency**	**Sector Coordinating Councils (SCCs)**	**Government Coordinating Councils (GCCs)**	**Regional Consortia**
Chemical	Department of Homeland Security	✓	✓	
Commercial Facilities ⓘ		✓	✓	
Communications ⓘ		✓	✓	
Critical Manufacturing		✓	✓	
Dams		✓	✓	
Emergency Services ⓘ		✓	✓	
Information Technology ⓘ		✓	✓	
Nuclear Reactors, Materials & Waste		✓	✓	
Food & Agriculture	Department of Agriculture, Department of Health and Human Services	✓	✓	
Defense Industrial Base ⓘ	Department of Defense	✓	✓	
Energy ⓘ	Department of Energy	✓	✓	
Healthcare & Public Health ⓘ	Department of Health and Human Services	✓	✓	
Financial Services ⓘ	Department of the Treasury	Uses separate coordinating entity	✓	
Water & Wastewater Systems ⓘ	Environmental Protection Agency	✓	✓	
Government Facilities	Department of Homeland Security, General Services Administration	Sector does not have an SCC	✓	
Transportation Systems ⓘ	Department of Homeland Security, Department of Transportation	Various SCCs are broken down by transportation mode or subsector.	✓	

Critical Infrastructure Cross-Sector Council

Federal Senior Leadership Council

State, Local, Tribal, and Territorial Government Coordinating Council

Regional Consortium Coordinating Council

ⓘ Indicates that a sector (or a subsector within the sector) has a designated information-sharing organization.

Source: Department of Homeland Security, "Table 1 – Sector and Cross-Sector Coordinating Structures," in *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, 2013, p. 12, https://www.nist.gov/system/files/documents/cybercommission/-DHS-_National_Infrastructure_Protection_Plan_-NIPP.pdf.

Notes: The Trump Administration dissolved the Critical Infrastructure Partnership Council in 2025, but coordinating bodies under its auspices continue to operate as of 2026 minus legal authorities for confidential deliberations between public and private-sector stakeholders. See the "Public-Private Partnership Coordination Bodies" section in the main text of this report.

Author Information

Brian E. Humphreys
Analyst in Science and Technology Policy

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.