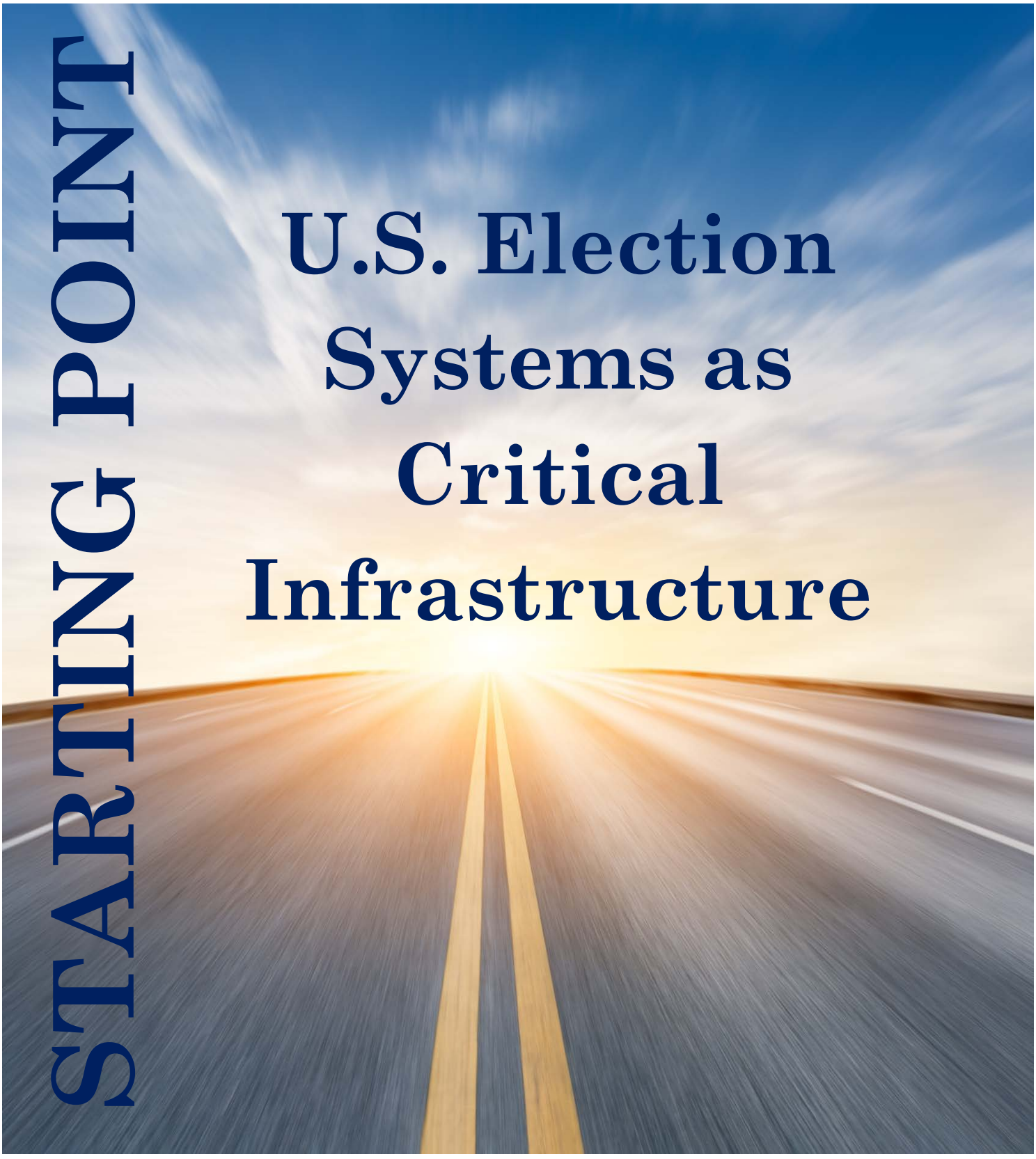
STARTING POINT

U.S. Election Systems as Critical Infrastructure



U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Starting Point:

U.S. Election Systems as Critical Infrastructure

On January 6, 2017, Department of Homeland Security (DHS) Secretary Jeh Johnson designated U.S. election systems as part of the nation's critical infrastructure, a decision that was later affirmed by current DHS Secretary John Kelly. Since the designation was announced, state and local election officials across the country have raised questions about the day-to-day impact of the designation and how it will benefit their work to conduct accessible, accurate and secure elections. This document details DHS's critical infrastructure designation and what election administrators can expect moving forward. It also provides a glossary of terms frequently used in conjunction with correspondence and discussions about the critical infrastructure designation.

What is critical infrastructure?

Critical infrastructure is a DHS designation established by the Patriot Act and given to "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." [i] DHS, the department responsible for critical infrastructure, was established by the Homeland Security Act in 2002.

In order to fulfill its responsibilities under the Patriot Act, DHS uses the National Infrastructure Protection Plan (NIPP) as the foundational document, or "rule book," for how to develop sector-specific critical infrastructure plans. The NIPP established a process roadmap by which the nation's critical infrastructure sectors can be identified and created.

In addition to the Patriot Act and NIPP, a third piece of critical infrastructure governing authority comes from Presidential Policy Directive 21 (PPD-21). Released on February 12, 2013, PPD-21 established the Federal Government's "strategic imperatives" in its approach to the nation's critical infrastructure. It established the current critical infrastructure sectors and identified each sector's Sector Specific Agency (SSA), which is the agency charged with structuring and managing the sector.

What other sectors are included in the nation's critical infrastructure?

Critical infrastructure sectors are groupings based on common function and form. There are currently 16 sectors. They are: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials and Waste; Transportation Systems; and Water and Wastewater Systems. [ii]

One critical infrastructure sector, Government Facilities, has three sub-sectors, Elections, National Monuments and Icons, and Education Facilities. Subsectors are sections of a specific sector that vary from the rest of the sector substantially enough to justify creating a plan just for the subsector.

How are sectors organized?

Once DHS creates a sector, the SSA structures it and helps it self-organize, a requirement of the NIPP. With regard to election systems, this means that members of the election community come together to join and manage the various components that make up this sector. After the critical infrastructure sector is formally established and organized, the SSA is charged with managing it. The SSA is "responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment." [iii]

While DHS has vast national security knowledge and resources, it acknowledges that it is not an issue-area expert for some of the sectors designated as critical infrastructure. To fill this knowledge gap, DHS will often appoint another federal agency as its Co- Sector Specific Agency (Co-SSA). This is especially common when DHS creates a subsector. Co-SSAs help DHS navigate the nuances of a specific subsector and share SSA responsibilities. For example, the sub-sector Co-SSA for Education Facilities is the Office of Safe and Drug-Free Schools in the Department of Education. A complete list of the sectors, and their respective SSAs and Co-SSAs follows at the end of this document (Addendum II).

DHS has yet to designate a Federal Agency as a Co-SSA for the elections sector. The U.S. Election Assistance Commission (EAC) has publicly called on DHS to select the commission to fill this important role. The request was made in light of the working relationship between DHS and the EAC, crafted during the 2016 presidential election and continued since.

Beyond the SSA and Co-SSA roles, there are other key entities established to support a newly designated critical infrastructure sector, including:

- ✓ **Sector Coordinating Councils (SCCs)**: These are "self-organized, self-run, and self-governed private sector councils consisting of owners and operators and their representatives, who interact on a wide range of sector-specific strategies, policies, activities, and issues. SCCs serve as principal collaboration points between the government and private sector owners and operators for critical infrastructure security and resilience policy coordination and planning and a range of related sector-specific activities." [iv]
- ✓ **Government Coordinating Councils (GCCs)**: These consist of "representatives from across various levels of government (including Federal and State, local, tribal and territorial), as appropriate to the operating landscape of each individual sector, these councils enable interagency, intergovernmental,

and cross-jurisdictional coordination within and across sectors and partner with SCCs on public-private efforts." [v]

As part of its designation plan, the SSA will work to establish these councils to support the U.S. election systems designation. For the U.S. election system, these groups will likely include representatives from federal, state, and local government; election system vendors; and other stakeholders impacted by the critical infrastructure designation.

Another key component of operating a critical infrastructure sector is to ensure clear, strong lines of communication between the SSA, Co-SSA, coordinating councils, and stakeholders. This can include creation of the following:

- ✓ **Information Sharing and Analysis Centers (ISACs)**: These are "operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders." (Source: Presidential Decision Directive 63, 1998)[vi]
- ✓ **Information Sharing and Analysis Organizations (ISAOs):** Though similar to ISACs, ISAOs are "any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of: (a) Gathering and analyzing Critical Infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof; (b) Communicating or disclosing Critical Infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to Critical Infrastructure or protected systems; and (c) Voluntarily disseminating Critical Infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (a) and (b)." [vii]

The distinction between an ISAC and an ISAO is that "[u]nlike ISACs, ISAOs are not directly tied to Critical Infrastructure sectors, as outlined in Presidential Policy Directive 21. Instead, ISAOs offer a more flexible approach to self-organized information sharing activities amongst communities of interest such as small businesses across sectors: legal, accounting, and consulting firms that support cross-sector clients, etc." [viii] Essentially, ISAOs allow for more widespread information sharing across sectors and among interested individuals regardless of clearance, knowledge level, or inclusion in a critical infrastructure sector.

What is unique about the protection of critical infrastructure communications?

Information about security and vulnerabilities that is shared under the restrictions of the Critical Infrastructure Information Act is considered Protected Critical Infrastructure Information (PCII). PCII is not subject to the many disclosure regulations, such as those found in the Freedom of Information Act and its state-level counterpart. This protection, allows the critical infrastructure community to discuss vulnerabilities and problems without publically exposing potentially sensitive information.[ix]

For those participating in election sector coordinating councils this protection means that some information communicated between DHS and the coordinating councils can be protected. This limits the potential for sensitive election security information to be made public and protects potentially sensitive material from being misconstrued or used for nefarious purposes. This protection is made possible by an exception to the Federal Advisory Committee Act created by the Critical Infrastructure Partnership Advisory Council.[x]

Are new resources available following a critical infrastructure designation?

A critical infrastructure designation provides for greater access to DHS information and security resources. It also provides a safer and more discreet exchange of information and requests for advice or assistance. While it is important to note that DHS will provide assistance to any domestic entity that requests help and not just critical infrastructure, its assistance to entities within a critical infrastructure sector is prioritized over providing assistance to non-critical infrastructure entities.

DHS resources – including on-going and current information about threats, risk and vulnerability assessments, and security best practices as well as hands-on advice – help infrastructure owners and managers better secure their systems. The department emphasizes the importance of the information assets it has available to critical infrastructure entities and understands that security clearances are a requirement for accessing some of these resources. This is why DHS works with infrastructure owners and managers to secure clearances when necessary.

Use of DHS resources and participation in sector councils is voluntary, and DHS continually states that it cannot force critical infrastructure owners and managers to interact with a sector, its components, or its resources. Entities that choose to leverage these new resources have a direct line to DHS resources via a Cyber Security and Protective Security Advisor. These advisors directly supply security assistance to the country and handle on-going assistance to CI entities.

While some within the election community remain skeptical about the critical infrastructure designation, their outstanding concerns about the designation make the case for why input from key election sector stakeholders is a vital part of setting up the needed infrastructure of councils and committees that can make this designation impactful. DHS is actively seeking participation from election stakeholders and their sector

allies, noting that there is an advantage inherent in helping to shape the critical infrastructure mechanisms election officials will use to gain resources and communicate with DHS. The department has relied on the EAC to provide the forum for much of this outreach, and the commission recommends that election officials and others in the election community take steps to becoming involved in this process either directly or through the EAC.

What role will the EAC play as DHS stands up the critical infrastructure designation?

The EAC has requested DHS name the commission as Co-SAA. This designation is important to ensure that state and local election officials and administrators have an informed federal advocate working directly with DHS as the department determines what resources and services are needed to protect U.S. election systems and how these resources will be distributed. The EAC has held and will continue to hold, hearings and meetings to give DHS a platform to discuss the designation and its potential benefits, as well as answer questions from stakeholders. The EAC prides itself on serving as a trusted intermediary between state and local election officials and federal government leaders, as well as a provider of resources needed to navigate this new space. Serving as the official Co-SSA for implementing the critical infrastructure designation would tap into this strength and provide election officials with assurance that their interests and concerns will shape the contours of DHS's plan moving forward.

Addendum I: Glossary of Key Terms and Acronyms

Critical Infrastructure Glossary

Critical Infrastructure	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. (Source:§1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e)))
Critical Infrastructure Partnership Advisory Council (CIPAC)	Council established by DHS under 6 U.S.C. §451 to facilitate effective interaction and coordination of critical infrastructure activities among the Federal Government, the private sector, and State, local, tribal and territorial governments. (Source: CIPAC Charter) These meetings are exempt from the Federal Advisory Committee Act (FACA) requirements that they be open to the public and provide meeting materials to the public.
Critical Infrastructure Sector	A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; NIPP 2013 addresses 16 critical infrastructure sectors, as identified in PPD-21. (Source: NIPP 2013: Partnering for Critical Infrastructure Security and Resilience)
Cybersecurity	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (Source: 2009 NIPP)
Executive Order 13636	Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity framework; and promote and incentivize the adoption of strong cybersecurity practices. (Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013)
Government Coordinating Council (GCC)	The government counterpart to the Sector Coordinating Council for each sector established to enable interagency and intergovernmental coordination; comprises representatives across various levels of government (Federal and State, local, tribal and territorial) as appropriate to the risk and operational landscape of each sector. (Source: 2009 NIPP)
Information Sharing and Analysis Centers (ISACs)	Operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders. (Source: Presidential Decision Directive 63, 1998) ISACs are not operated, controlled, or managed by DHS.

Information Sharing and Analysis Organization (ISAO)	"Any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability there of; communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure or protected systems; and voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B)." (Source: Homeland Security Act of 2002)
Infrastructure	The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole; consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (Source: DHS Lexicon, 2010)
National Annual Report	Each SSA is required to provide an annual report to the Secretary of Homeland Security on their efforts to identify, prioritize, and coordinate CI/KR protection in their respective sectors. (National Infrastructure Protection Plan: The National CI/KR Protection Annual Report)
National Infrastructure Coordinating Center (NICC)	The National Infrastructure Coordinating Center (NICC) is the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government. When an incident or event affecting critical infrastructure occurs and requires coordination between the Department of Homeland Security and the owners and operators of our nation's infrastructure, the NICC serves as that information sharing hub to support the security and resilience of these vital assets. (Source: DHS.gov/national-infrastructure-coordinating-center)
National Infrastructure Protection Plan (NIPP)	The National Infrastructure Protection Plan 2013, involving stakeholders from all 16 critical infrastructure sectors, all 50 states, and from all levels of government and industry, provides a clear call to action to leverage partnerships, innovate for risk management, and focus on outcomes, provides an updated approach to critical infrastructure security and resilience, and involves a greater focus on integration of cyber and physical security efforts. (DHS, NIPP Fact Sheet)
National Protection and Programs Directorate (NPPD) – (DHS/NPPD)	[The DHS division] that leads the DHS mission to reduce risk to the Nation's critical physical and cyber infrastructure through partnerships that foster collaboration and interoperability. (Source: DHS FY13 Budget Guidance). NPPD contains the Federal Protective Service, the Office of Identity Management, the Office of Cybersecurity and Communications, the Office of Cyber and Infrastructure Analysis, and the Office of Infrastructure Protection.

Presidential Policy Directive 21 (PPD-21)	[Presidential Directive that] Aims to clarify roles and responsibilities across the Federal Government and establish a more effective partnership with owners and operators and State, local, tribal and territorial entities to enhance the security and resilience of critical infrastructure. (Source: PPD-21, 2013)
Presidential Policy Directive 8 (PPD-8)	[Presidential Directive that] facilitates an integrated, all-of-Nation approach to national preparedness for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters; directs the Federal Government to develop a national preparedness system to build and improve the capabilities necessary to maintain national preparedness across the five mission areas covered in the PPD: prevention, protection, mitigation, response, and recovery. (Source: PPD-8, 2011)
Protected Critical Infrastructure Information (PCII)	PCII is [information and communications] protected from disclosure. All critical infrastructure information that has been properly submitted and validated pursuant to the Critical Infrastructure Information Act and implementing directive; all information submitted to the PCII Program Office or designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise. Critical infrastructure information voluntarily shared with the government and validated as PCII by the Department of Homeland Security is protected from, the Freedom of Information Act (FOIA), State, local, tribal, and territorial disclosure laws, use in regulatory actions and use in civil litigation. PCII can only be accessed in accordance with strict safeguarding and handling requirements, and only trained and certified federal, state, and local government employees or contractors may access PCII.(Source: CII Act of 2002, 6 U.S.C. § 131, and www.dhs.gov/pcii-program)
Protective Security Advisors (PSAs)	Trained critical infrastructure protection and vulnerability mitigation subject matter experts who work for DHS and are responsible for ensuring all Office of Infrastructure Protection critical infrastructure security and resilience programs and services are delivered to State, local, tribal, and territorial stakeholders and private sector owners and operator. There are three types: (1) Regional Directors, supervisory PSAs, PSAs, and geospatial analysts. s. (Source: DHS.gov/protective-security-advisors)
Sector Coordinating Council (SCC)	The private sector counterpart to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. They serve as principal entry points for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. (Source: Adapted from the 2009 NIPP)
Sector-Specific Agency (SSA)	A Federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise, as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (Source: PPD-21, 2013)

Sector-Specific Plans (SSP)	Planning documents that complement and tailor application of the National Infrastructure Protection Plan to the specific characteristics and risk landscape of each critical infrastructure sector. SSPs are developed by the SSAs in close collaboration with the SCCs and other sector partners. (Source: Adapted from the 2009 NIPP)

Addendum II: Critical Infrastructure Sectors and their SSAs and Co-SSAs

Sector/ Subsector	SSA	Co-SSA
Chemical	Department of Homeland Security (DHS)	
Commercial Facilities	Department of Homeland Security (DHS)	
Communications	Department of Homeland Security (DHS)	
Critical Manufacturing	Department of Homeland Security (DHS)	
Dams	Department of Homeland Security (DHS)	
Defense Industrial Base	Department of Defense (DOD)	
Emergency Services	Department of Homeland Security (DHS)	
Energy	Department of Energy (DOE)	
Financial Services	Department of the Treasury	
Food and Agriculture	Department of Agriculture (USDA)	Department of Health and Human Services (HHS)
Government Facilities	Department of Homeland Security (DHS)	General Services Administration (GSA)
Elections (subsector)	Department of Homeland Security (DHS)	
Education Facilities (subsector)	Department of Homeland Security (DHS)	Department of Education
National Monuments (subsector)	Department of Homeland Security (DHS)	Department of the Interior (DOI)
Healthcare and Public Health	Department of Health and Human Services (HHS)	
Information Technology	Department of Homeland Security (DHS)	
Nuclear Reactors, Materials, and Waste	Department of Homeland Security (DHS)	
Transportation Systems	Department of Homeland Security (DHS)	Department of Transportation (DOT)
Water and Wastewater Systems	Environmental Protection Agency (EPA)	

[i] Patriot Act, (Sec. 1016(e))
[ii] https://www.dhs.gov/Critical-Infrastructure-sectors, accessed May 2, 2017.
[iii] Ibid.
[iv] Department of Homeland Security, *National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience*, p. 12.
[v] *NIPP 2013*, p. 31.
[vi] Presidential Decision Directive 63, 1998.
[vii] Source: *Homeland Security Act of 2002, 6 U.S.C. § 131.*
viii Department of Homeland Security, Frequently Asked Questions About Information Sharing and Analysis Organizations (ISAOs), https://www.dhs.gov/isao-faq, accessed May 3, 2017.
[ix] Department of Homeland Security, *NIPP 2013*, p. 12.
[x] Department of Homeland Security, *United States Department of Homeland Security Charter of the Critical Infrastructure Partnership Advisory Council,* https://www.dhs.gov/sites/default/files/publications/cipac-charter-11-30-16-508.pdf, accessed June 5, 2017