Table of Contents

1. INTRODUCTION

The Nation's critical infrastructure provides vital services that underpin our society; managing risks to this infrastructure is essential to America' security and resilience. *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience* (hereafter referred to as the *National Plan),* guides the National efforts to manage risk to the Nation's critical infrastructure. Fundamental to this effort is the identification of national priorities, clearly articulated goals, measurements of progress, and means for continuous improvement. It relies on a spectrum of capabilities, expertise, and experience within and throughout the critical infrastructure community.

This *National Plan* builds on and supersedes the 2009 *National Infrastructure Protection Plan* and recognizes the valuable progress made to date to protect the Nation's critical infrastructure. It is written cognizant of changes in the risk, policy and operating environments; and is informed by the need to integrate the cyber, physical and human elements of critical infrastructure risk management. The scope of the *National Plan* is to guide national efforts, drive progress, and engage the broader community about the importance of critical infrastructure security and resilience.

The audience for this plan includes a broad critical infrastructure community comprised of public and private critical infrastructure owners and operators; Federal departments and agencies (to include Sector Specific Agencies); State, local, tribal and territorial (SLTT) governments; regional entities; and other private and non-profit organizations with a role to play in securing and strengthening the resilience of critical infrastructure.

Managing risks to critical infrastructure requires an integrated approach across this broad community to:

- Detect, deter, disrupt, and prepare for threats to the Nation's critical infrastructure, including natural hazards;
- Reduce vulnerabilities of critical assets, systems, and networks; and,
- Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.

Given the diverse authorities, roles, and responsibilities of the critical infrastructure partners, flexible, proactive, and inclusive partnerships are required to advance critical infrastructure security and resilience. Presidential Policy Directive 21 (PPD-21) notes, "Critical infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient." Individual efforts to manage risk are strengthened by a collaborative public-private partnership characterized by unified national effort, as opposed to a hierarchical, command-and-control structure. It is built on a trusted environment, where processes for information sharing improve situational awareness, and remain open and transparent while protecting privacy and civil liberties.

The *National Plan* takes into account the varying risk management perspectives of the public and private sectors, where government and private industry have aligned, but not identical, interests in securing critical infrastructure. It leverages comparative advantages of both the private and

public sectors to the mutual benefit of all. The *National Plan* is organized in the following manner:

- **Section 2 – Vision, Mission, and Goals** – Outlines the vision, mission, and goals for the critical infrastructure community.
- **Section 3 – Critical Infrastructure Environment** – Describes key concepts influencing security and resilience efforts with a focus on the policy, risk, and operating environments and the partnership structure.
- **Section 4 – Core Tenets** – Describes the principles and assumptions that underpin the development of this National Plan
- **Section 5 – Collaborating to Manage Risk** – Describes a common framework for risk management activities conducted by the critical infrastructure community in the context of national preparedness.
- **Section 6 – Call to Action** – Calls upon the Federal government, in partnership with the critical infrastructure community (respective of authorities, responsibilities, and business environments), to take cross-cutting actions that support collective efforts in critical infrastructure security and resilience in the coming years.
- **Glossary of Terms**
- **Appendices – The Partnership Approach; Roles, Responsibilities and Capabilities of Critical Infrastructure Partners and Stakeholders**

Several supplemental resources are also offered to provide guidance and assistance to the critical infrastructure community as part of implementing the *National Plan.* These supplements are intended to be standalone resources; additional supplements will continue to be developed after the *National Plan* has been issued. At the time of this release, supplemental resources include:

- Implementing the Critical Infrastructure Risk Management Framework
- Connecting to the National Cybersecurity and Communications Integration Center (NCCIC) and the National Infrastructure Coordinating Center (NICC).
- U.S. Department of Homeland Security (DHS) Resources for Vulnerability Assessments
- Incorporating Security and Resilience into Critical Infrastructure Projects

Evolution from the 2009 NIPP

The *National Plan* retains a focus on risk management as the foundation of critical infrastructure security and resilience and continues to promote partnerships as the key mechanism through which risks are managed. In doing so, it reaffirms the role of various coordinating structures including Sector Coordinating Councils, Government Coordinating Councils, and cross-sector councils. Building on progress made toward critical infrastructure security and resilience by those councils and others over the past 15 years, this *National Plan* reflects the following evolution from the 2009 *NIPP*:

- Elevates security and resilience as the primary aim of critical infrastructure planning efforts;

- Expands and updates critical infrastructure risk management to address alignment to the National Preparedness System, across the prevention, protection, mitigation, response and recovery mission areas;
- Focuses on national priorities jointly determined by public and private sector, while limiting discussion of Federal programs;
- Integrates cyber and physical security and resilience efforts into an enterprise approach to risk management;
- Affirms the reality that critical infrastructure security and resilience efforts require international collaboration;
- Continues progress to support execution of the *National Plan* at both the national and community levels; and
- Presents a detailed Call to Action, including steps the Federal government will undertake– working with critical infrastructure partners – to make progress toward security and resilience.

2. VISION, MISSION, AND GOALS

The strategic direction for efforts to build and sustain critical infrastructure security and resilience is driven by common vision, mission and goals:

Vision

A Nation in which physical and cyber critical infrastructure remains secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery is hastened

The vision above can be achieved through the fulfillment of the following mission:

Mission

Strengthen the security and resilience of the Nation's critical infrastructure, through the collaborative and integrated efforts of the critical infrastructure community by managing risks, whether physical or cyber

Goals

The vision and mission depend on the achievement of goals that represent the strategic direction in which critical infrastructure activities should be focused over the next several years.

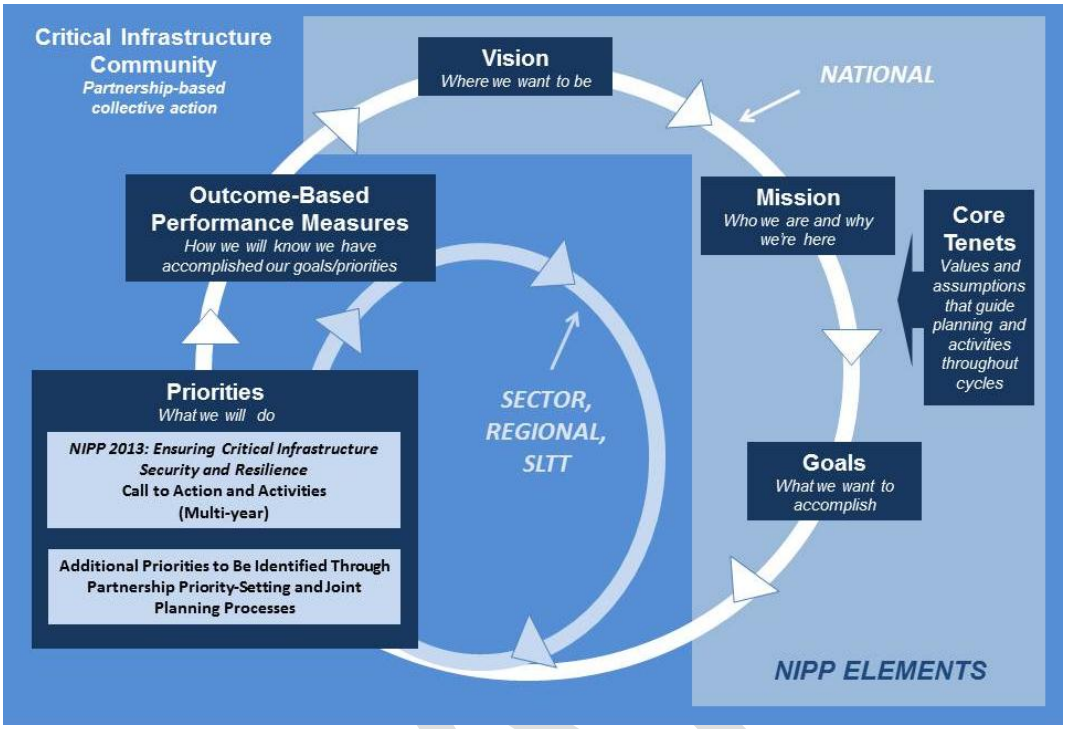
- ***Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities;***
- ***Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;***
- ***Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation, as well as effective responses to both save lives and ensure the rapid recovery of essential services;***
- ***Efficiently share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and***
- ***Promote learning and adaptation during and after exercises and incidents.***

These goals will be augmented by the regular development of more specific priorities by the critical infrastructure partnership.

Based on the vision, mission and goals, the critical infrastructure community will work jointly to set national priorities, while considering resource availability, progress already made, known capability gaps, and emerging risks. These priorities should drive action nationally and will be supplemented by sector, regional, and SLTT priorities.

Performance measures will be set based on the goals and priorities. The results of annual measurement of progress, as reflected in the National Annual Report and the National Preparedness Report, will help build a common understanding of the state of critical infrastructure security and resilience efforts. The interrelationship of these elements is depicted in Figure 1 below.

Figure 1. The NIPP's Approach to Building and Sustaining Unity of Effort for Critical Infrastructure Security and Resilience



3. CRITICAL INFRASTRUCTURE ENVIRONMENT

This *National Plan* relies on several key definitional concepts, which remain consistent with the previous NIPP. At the same time, the Plan is informed by and updated as a result of the evolving critical infrastructure risk, policy, and operating environment. This section describes changes and evolution of the critical infrastructure environment that have occurred since the publication of the last NIPP while affirming the importance of the core partnership structure that enables successful collaboration to manage risks.

Key Concepts

Several key concepts are defined below to provide context for this critical infrastructure environment. An understanding of these key concepts influences the state of critical infrastructure and shapes the community's approach to ensuring security and resilience.

- **Critical infrastructure** represents "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."[1] Presidential Policy Directive 21 (PPD-21) further states that critical infrastructure "provides essential services that underpin American society" and notes that critical infrastructure "includes distributed networks, varied organizational structures and operating models (including multinational and international ownership), interdependent functions and systems in both the physical

[1] USA Patriot Act of 2001(42 U.S.C. 5195c(e)), section 1016(e)

space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations."[2] The Nation's critical infrastructure is largely owned and operated by the private sector, however Federal, State, local, tribal, and territorial governments also own and operate critical infrastructure, as do foreign entities with reach into the U.S.

- PPD-21 defines **security** as "reducing the risk to critical infrastructure by physical means or defens[ive] cyber measures to intrusions, attacks, or the effects of natural or manmade disasters." There are several elements of securing critical infrastructure systems, including preventing and protecting against incidents and sharing accurate information and analysis on current and future risks. Prevention and protection are important missions to support critical infrastructure security.
- **Resilience**, as defined in PPD-21, is "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions...[it] includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents." As with building security, having accurate information and analysis about risk is essential to achieving resilience. Resilient infrastructure assets, systems, and networks, must also be robust, agile, and adaptable. Mitigation, response, and recovery are important missions to support critical infrastructure resilience.
- Security and resilience are strengthened through risk management. **Risk** refers to the "potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood [a function of threats and vulnerabilities] and the associated consequences"; and **risk management** is the "process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost."[3]
- **Partnership** enables more effective and efficient risk management. Within the context of this plan, it is defined as close cooperation between parties having common interests in achieving a shared vision. For the critical infrastructure community, leadership involvement, open communications, and trusted relationships are essential elements to partnership.

Risk Environment

The risk environment affecting critical infrastructure is complex and uncertain; threats, vulnerabilities, and consequences have all evolved over the last 10 years. For example, the increasing development of information and communications technologies, and its use to operate critical infrastructure combined with enhanced focus of exploiting that technology has altered the cyber risk environment dramatically.

Threats must be considered from an all-hazards perspective. The Strategic National Risk Assessment[4] (SNRA) defines numerous threats to homeland security in the broad categories of adversarial/human-caused, natural, and technological/accidental threats. Critical assets, systems, and networks face many of the threats categorized by the SNRA, including terrorists and other

[2] The White House, Presidential Policy Directive 21 -- Critical Infrastructure Security and Resilience, 12 February 2013, accessed 24 September 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[3] DHS Risk Lexicon – 2010 Edition, September 2010, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

[4] Department of Homeland Security, Strategic National Risk Assessment, December 2011, http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf

adversarial actors seeking to cause harm and disrupt essential services through physical and cyber attacks, severe weather events, pandemic influenza or other health crises, and the potential for accidents and failures due to infrastructure operating beyond its intended lifespan. In addition, the potential for interconnected events with unknown consequences add uncertainty in addition to known risks analyzed as part of the SNRA.

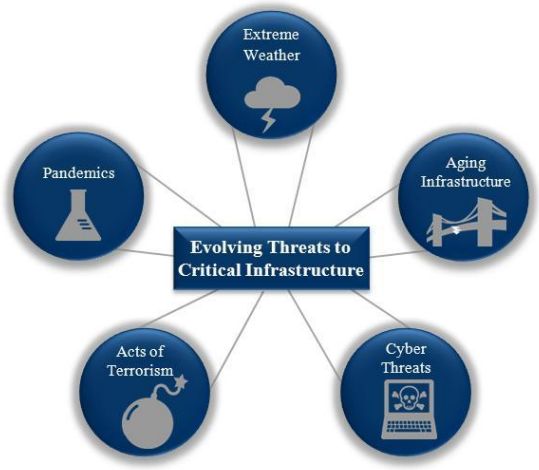


Figure 2: Evolving Threats

Growing interdependencies across critical infrastructure systems, particularly reliance on information and communications technologies, have heightened the vulnerability to physical and cyber threats and potential consequences resulting from the compromise of underlying systems or networks. In an increasingly interconnected world, where critical infrastructure crosses international borders and global supply chains, the impact of these threats is exacerbated.

Additionally, the effects of extreme weather pose a growing risk to critical infrastructure – rising sea levels, more severe storms, extreme and prolonged drought conditions, and severe flooding combine to threaten infrastructure that provides essential services to the American public. Ongoing and future changes to the climate have the potential to exacerbate these risks and could have major impact on infrastructure operations.

Finally, where skill gaps may exist as a result of a retiring work force or lack of skilled labor, the resulting gaps can also result in vulnerabilities. Skilled operators are necessary for infrastructure maintenance and, therefore, security and resilience. These various factors influence the risk environment, creating (along with the policy and operating environments) the back drop in which decisions are made for critical infrastructure security and resilience.

Policy Environment

Title II of the Homeland Security Act of 2002 (as amended) provides the basis for the Department of Homeland Security's (DHS) responsibilities in the area of critical infrastructure security and resilience. The Act also specifically calls for DHS to develop a comprehensive Plan for securing the Nation's critical infrastructure. DHS completed the first version of the *NIPP* in 2006, and issued an update in 2009. Since 2009, numerous national policies have continued to shape the way the Nation addresses critical infrastructure security and resilience and national preparedness.

On February 12, 2013, the President issued PPD-21, *Critical Infrastructure Security and Resilience,*[5] which explicitly calls for the development of an updated *National Plan*. The directive builds on the extensive work conducted to protect critical infrastructure, and describes the Nation's emphasis on identifying and disrupting threats, reducing vulnerabilities, minimizing

[5] The White House, Presidential Policy Directive 21 -- Critical Infrastructure Security and Resilience, 12 February 2013, accessed 6 August 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

consequences, and hastening response and recovery efforts related to critical infrastructure. PPD-21 also identifies energy and communications systems as uniquely critical due to the essential services they provide across all critical infrastructure sectors. Overall, it identifies 16 critical infrastructure sectors[6]: 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.

To recognize and manage risk introduced by the increasing reliance of critical infrastructure on information and communications technology, the President also issued Executive Order 13636: *Improving Critical Infrastructure Cybersecurity*. EO 13636 calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to "improve cybersecurity information sharing and collaboratively develop and implement risk-based" approaches to cybersecurity.[7] To that end, the executive order directs the Federal Government to develop a technology-neutral cybersecurity framework to reduce cyber risk to critical infrastructure; promote and incentivize the adoption of strong cybersecurity practices; increase the volume, timeliness, and quality of information sharing related to cyber threats; and incorporate protection for privacy and civil liberties into critical infrastructure security and resilience initiatives.

In addition critical infrastructure security and resilience efforts to manage risk must align with efforts to enhance the Nation's overall level of preparedness. To that end, the *National Plan* is consistent with PPD-8, *National Preparedness*, which identifies five mission areas—prevention, protection, mitigation, response, and recovery—that are central to comprehensively enhancing national preparedness. As part of PPD-8, a National Preparedness Goal was developed to represent the country's common focus. The *National Plan* helps achieve PPD-8's National Preparedness Goal namely "a secure and resilient Nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."

Operating Environment

Critical infrastructure security and resilience remain central focus areas within homeland security. The Nation has benefited from the investments made by both owners and operators and the public sector in increased security and resilience. Much of the critical infrastructure community continues to integrate cybersecurity into core business practices, making significant investments to increase security and resilience. In other areas, however, further investment is needed to keep pace with change as indicated in the American Society of Civil Engineers (ASCE) Report Card for infrastructure.[8] The report highlights the improvement in overall

[6]The White House, Presidential Policy Directive -- Critical Infrastructure Security and Resilience, 12 February 2013, accessed 6 August 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[7] The White House, Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, 12 February 2013, accessed 22 August 2013, http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[8] Every 4 years, the ASCE releases a report card for America's Infrastructure that depicts the condition and performance of the nation's infrastructure by assigning letter grades to each type of infrastructure. In its 2013 Report Card for America's Infrastructure, ASCE graded the country's overall infrastructure at a D+. The grades in 2013 ranged from a high of B- for solid waste to a low of D- for levees and waterways. Overall the report found that solid waste, drinking water, wastewater, roads, and bridges all saw incremental improvements, and rail jumped from a C-

infrastructure from a D- to a D+ and emphasizes there were no drops in grades. The report card also emphasizes that more work and investment is needed in (largely publicly-funded) infrastructure assets at risk due to age, maintenance, and changing operating conditions.

The extent to which infrastructure is interconnected shapes the environment for critical infrastructure security and resilience by necessitating collaboration in both planning and activities. The Nation's critical infrastructure has become much more interdependent, continuing to move from an operating environment characterized by disparate systems, assets, and networks to a system where cloud computing, mobile devices, and wireless connectivity have dramatically changed the how infrastructure is operated. Interdependencies can be operational (e.g., power required to operate a water pumping station) or physical (e.g., co-located infrastructure, such as water and electric lines running under a bridge span). Interdependencies can be extremely narrow or span vast regions, crossing jurisdictional and national boundaries. One example of these dependencies is highlighted in infrastructure systems, assets, and networks with the need for accurate and precise positioning, navigation and timing (PNT) data. These services are critical to the operations of multiple critical infrastructure sectors and are vital to incident response.

Critical infrastructure systems, assets, and networks, as well as other key resources, reside in particular jurisdictions, but their resulting information, products, services, and functions can be provided worldwide. The nature of critical infrastructure ownership and operations is also distributed, and the need for joint planning and investment is becoming more common and necessary on the international, national, and regional levels. This informs the way that the critical infrastructure community should plan to work together, within and across sectors, and across jurisdictions and international borders, to increase the security and resilience of critical infrastructure.

Finally, information security and privacy considerations also shape the operating environment. The increasing availability of data and information essential to operating and maintaining infrastructure and related technologies has both fundamentally changed and enabled more efficient and effective practices. This information is vulnerable to unauthorized access that could affect its confidentiality, integrity, or availability. The distribution of such information to those entities that can use it for efficient and effective risk management practices remains a challenge. Critical to the success of maintaining the availability of information and distributing to those that can use it is transparency about the information sharing practices conducted; protection of sources and methods; ensuring privacy and civil liberties; and also enabling law enforcement investigations.

The complex and dynamic risk and operating environment underscore the challenge in securing and strengthening the resilience of the Nation's critical infrastructure. The environment shapes and influences the decisions made for both public and private entities. Because of the dynamic nature of this environment, the ability to partner for critical infrastructure security and resilience to take advantage of unique skills and capabilities across the community remains the key mechanism to achieve results. The partnership structure established in the 2006 NIPP enables

---

to a C+. Since 1998, the ASCE has graded the nation's major infrastructure categories at near failing, due to delayed maintenance and underinvestment across the majority infrastructure categories. American Society for Civil Engineers, 2013 Report Card for America's Infrastructure, http://www.infrastructurereportcard.org/

such partnership to occur and remains valid and the foundation for collaborating to achieve results.

Partnership Structure

Voluntary collaboration between private sector owners and operators (including their partner associations, vendors, and others) and government entity counterparts has been and will remain the primary mechanism for advancing national critical infrastructure security and resilience efforts. Many sectors have worked to establish stable and representative partnerships, managing transitions in leadership and broadening the range of members and skill sets needed to accomplish collective goals.

As the nature of the critical infrastructure risk environment precludes any one entity from managing risks entirely on its own, partners have benefitted from access to knowledge and capabilities that would otherwise not be available to them. Additionally, through trusted relationships and information-sharing, Federal agencies have gained a better understanding of the risks facing critical infrastructure, as well as its preparedness posture. This allows for more informed efforts to identify and address national critical infrastructure priorities.

The partnership approach provides the foundational structures for effective collaboration on critical infrastructure security and resilience. Participation in this effort is based on a clear national shared interest in ensuring the security and resilience of the Nation's critical infrastructure and an understanding of the comparative advantage each element of the partnership can bring to achieve this shared interest.

The *National Plan* relies on the organization of critical infrastructure into 16 sectors with the continued designation of a Federal department or agency as the lead coordinator for each sector, identified as Sector-Specific Agencies ((SSAs), refer to Appendix B for Roles and Responsibilities). The sector and cross-sector partnership council structures described in previous NIPPs remain the foundation for this *National Plan* and are depicted in Figure 3.

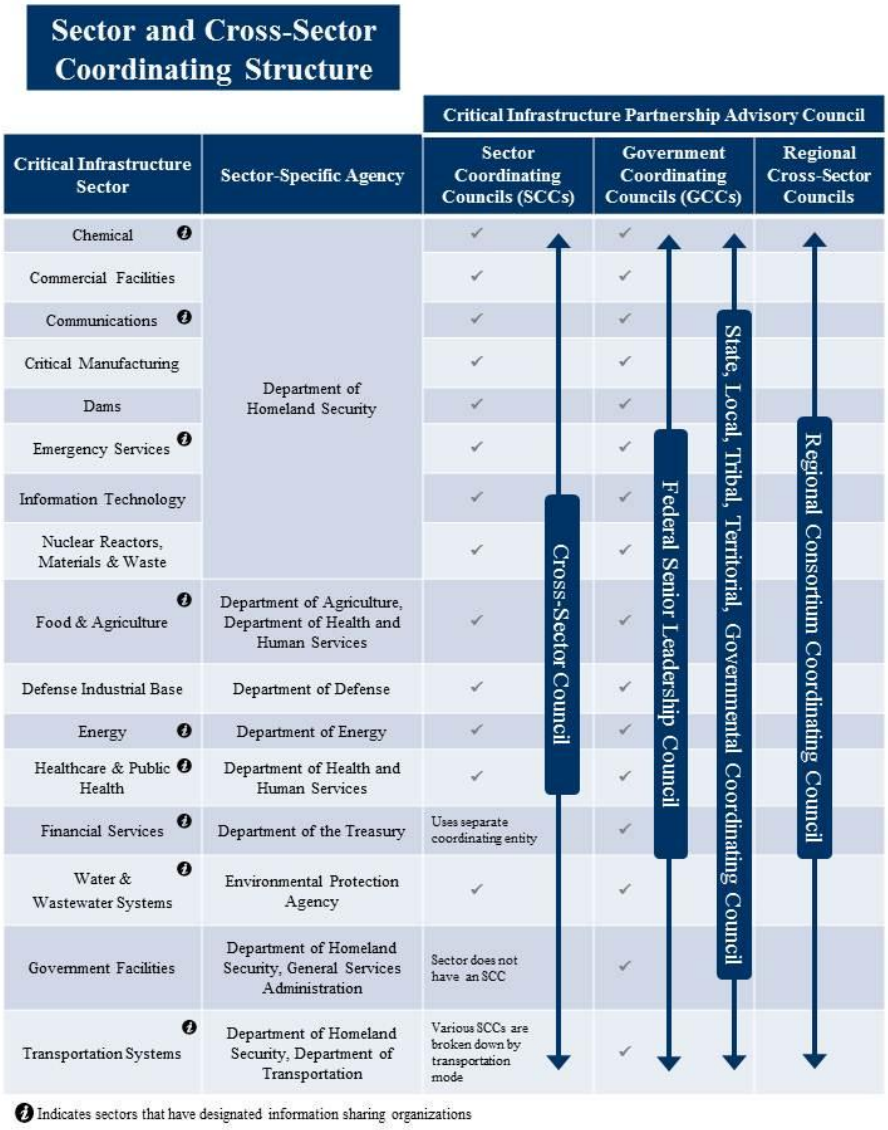


Figure 3: Sector and Cross-Sector Partnership Council Structure

These sector and cross-sector council structures include:

- Sector Coordinating Councils (SCCs) – self forming, self-organizing, and self-governing private sector councils that enable owners and operators and their representatives to interact on a wide range of sector-specific strategies, policies, activities, and issues. SCCs are recognized by the Federal government to serve as the principal collaboration points between the government and private sector owners and operators for sector policy coordination and planning and a range of sector-specific critical infrastructure security and resilience activities.
- Critical Infrastructure Cross-Sector Council – comprises the leadership of the SCCs. The private sector cross-sector council coordinates cross-sector issues, initiatives, and interdependencies to support critical infrastructure security and resilience.

- Government Coordinating Councils (GCCs) – comprise representatives from across various levels of government (including Federal and SLTT), as appropriate to the operating landscape of each individual sector. GCCs enable interagency, intergovernmental, and cross-jurisdictional coordination within and across sectors and partner with SCCs public-private efforts.
- Federal Senior Leadership Council (FSLC) – comprises the leadership of the SSAs and other Federal departments and agencies with a role in critical infrastructure security and resilience. The FSLC facilitates communication and coordination on critical infrastructure security and resilience across the Federal Government.
- State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) – comprises representatives from across SLTT government entities. The SLTTGCC promotes the engagement of SLTT partners in national critical infrastructure security and resilience efforts and provides an organizational structure to coordinate across jurisdictions on State and local government guidance, strategies, and programs.
- Regional Consortium Coordinating Council (RC3) – comprises regional groups and coalitions around the country engaged in various initiatives to advance critical infrastructure security and resilience in the public and private sectors.
- Information Sharing Organizations – organizations including Information Sharing and Analysis Centers (ISACs) serve operational and dissemination functions for many sectors and sub-sectors, and other groups, and facilitate sharing of information between government and the private sector.

Note: The functions of the above partnership structure, as well as additional structures that support national critical infrastructure security and resilience are further described in Appendix A.

Many of these structures take advantage of the Critical Infrastructure Partnership Advisory Council (CIPAC).[9] CIPAC was established by the Secretary of Homeland Security in 2006 as a mechanism to directly support sectors' interest to jointly engage in critical infrastructure discussions and to participate in a broad spectrum of activities. CIPAC is a specific mechanism available to convene the public-private critical infrastructure community by exempting partnership meetings from the Federal Advisory Committee Act (FACA).[10] Specifically, CIPAC forums serve advisory roles to the Federal government by supporting deliberations on critical infrastructure issues that are needed to arrive at a consensus position or when making formal recommendations. CIPAC may also be used at the sector, cross-sector, or working group level, depending on the topic and deliberation purpose. Other Federal agencies may also have FACA-exempt committees and advisory councils to engage with the private sector; however the CIPAC model provides the legal framework for cross-sector collaboration.

Partnering and planning must not only occur at the national level, but also across critical infrastructure communities. The sector- and cross-sector partnership approach described above is designed to be scalable and allow individual owners and operators of critical infrastructure and

[9] Critical Infrastructure Partnership Advisory Council. http://www.dhs.gov/critical-infrastructure-partnership-advisory-council

[10] Pub.L. 92–463, 6 October 1972.

other stakeholders across the country to participate. It is intended to promote consistency of process to enable efficient collaboration between disparate parts of the critical infrastructure community, while allowing for the use of other identified viable partnership structures and planning processes. This concept has proven successful and can be leveraged at the State, local, tribal, territorial levels as well as within and across regions to build, form or expand existing networks; identify proven practices; adapt to or adopt lessons-learned; and leverage practices, processes or plans as appropriate.

The partnership structure discussed above forms the basis (within the context of the risk, policy and operating environment) to collaborate and guide collective efforts to address critical infrastructure security and resilience efforts. This *National Plan* is informed and written within the context of this challenging and diverse environment and is guided by a set of core tenets focused on aspects of risk management and partnering.

4. CORE TENETS

The *National Plan* establishes seven core tenets that should influence planning related to critical infrastructure security and resilience. They represent the values and assumptions that should be considered at the national, regional, SLTT, and owner and operator levels in future planning for critical infrastructure security and resilience.

1. **Risk should be managed in a coordinated and comprehensive way across the critical infrastructure community to enable the effective allocation of security and resilience resources.**

Collaboratively managing risk minimizes duplication of effort and requires sharing information (including smart practices), thus promoting more efficient and effective use of resources. It also enables the development and execution of more comprehensive measures to detect, deter, disrupt, and prepare for threats; mitigate vulnerabilities; and reduce consequences across the Nation. To ensure a comprehensive approach to risk management, treatment of it must account not only for risk mitigation, but also other ways to address risk, including acceptance, avoidance, or transference.

2. **Understanding and addressing risks resulting from cross-sector dependencies and interdependencies are essential to enhancing critical infrastructure security and resilience.**

The way infrastructure sectors interact, including through reliance on shared information and communications technologies (i.e. cloud services), shapes how the Nation's critical infrastructure partners should collectively manage risk. For example, all critical infrastructure sectors rely on functions provided by energy and communications systems, as well as transportation systems and water and wastewater systems, among others. Additionally, interdependencies flow both ways, as with the dependence of the energy and communications systems on each other and other functions. It is important for the critical infrastructure community to understand and appropriately account for dependencies and interdependencies when managing risk.

3. **Gaining knowledge of infrastructure interdependencies, consequences, and risk requires information sharing across the critical infrastructure community.**

Through their operations and perspectives, stakeholders across the critical infrastructure community possess and produce diverse information necessary to the enhancement of critical

infrastructure security and resilience. Sharing and jointly planning based on this information is imperative to comprehensively addressing critical infrastructure security and resilience in an environment of increasing interconnectivity. For that to happen, legal protections, trusted relationships, enabling technologies, and consistent processes must be in place.

4. The partnership approach to critical infrastructure security and resilience recognizes the unique perspective and comparative advantage of the diverse critical infrastructure community.

The public-private partnership is the foundation for maintaining critical infrastructure security and resiliency. A well-functioning partnership depends on a defined purpose for its activities, articulated goals and measurable outcomes to guide shared activities, leadership involvement, clear and frequent communication, flexibility, adaptability, and trust. All levels of government, private and nonprofit sectors bring unique expertise, capabilities, and core competencies to the effort of ensuring critical infrastructure is secure and resilient. Recognizing the value of different perspectives helps the partnership more distinctly understand challenges and solutions related to critical infrastructure security and resilience. Identifying and recognizing each organization's values, roles, and responsibilities as part of the partnership, in a way that is respectful of unique perspectives, capabilities and resources informs a greater unity of effort to reduce security and resilience gaps.

5. Regional and SLTT partnerships are crucial to developing shared perspectives on gaps and actions to improve critical infrastructure security and resilience.

The *National Plan* emphasizes an approach to achieving security and resilience by partnering across institutions geographies. Risks have local consequences making it essential to execute initiatives on a regional-scale in a way that complements and operationalizes the national effort. This requires public, private, and non-profit organizations provide their perspectives in the assessment of risk and mitigation strategies. Local partnerships throughout the country augment the efforts of existing partnerships at the national level and are essential to achieving a true national effort.

6. Infrastructure critical to the United States transcends national boundaries, requiring cross-border collaboration, mutual assistance, and other cooperative agreements.

The United States benefits from and depends upon a global network of infrastructure that enables the Nation's security and way of life. The distributed nature and interconnectedness of these systems, assets, and networks have created a complex environment in which the risks the Nation faces are not distinctly contained within its borders. This is increasingly the case as services provided by critical infrastructure in many cases are dependent on information gathered, stored, or processed in highly distributed locations. It is imperative that the government, private sector, and international partners work together. This includes working together to fully understand supply chain vulnerabilities and implement coordinated – and not competing -- global security and resilience measures.

7. Security and resilience should be considered during the design of systems, assets, and networks

As critical infrastructure is built and refreshed, those involved in making design decisions, including those related to control systems, should consider the most effective and efficient ways to detect, deter, disrupt, and prepare for threats; mitigate vulnerabilities; and minimize

consequences. This includes considering infrastructure resilience principles, which are described in a supplement to this document, titled "Incorporating Security and Resilience into Critical Infrastructure Projects."

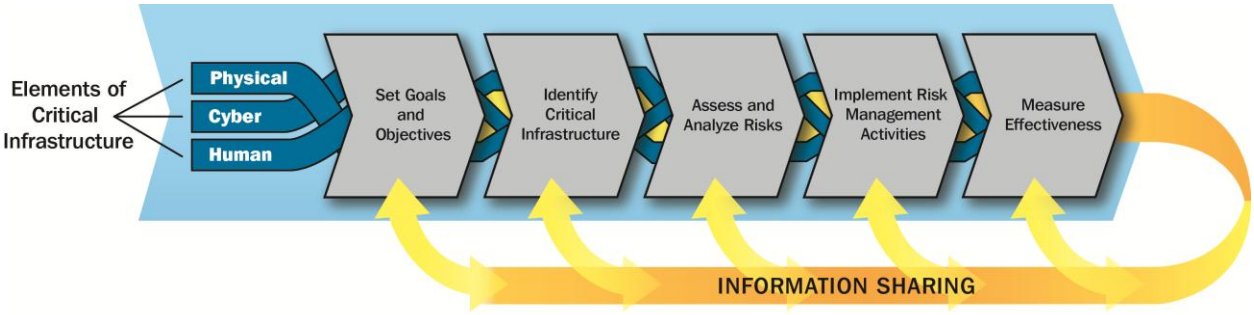
5. COLLABORATING TO MANAGE RISK

The national effort to strengthen critical infrastructure security and resilience depends on the ability of public and private sector critical infrastructure owners and operators to make risk-informed decisions when allocating limited resources in both steady-state and crisis operations. Therefore, risk management is the cornerstone of the *National Plan* and is relevant at the national, regional, State, and local levels. National, regional, and local resilience is dependent upon creating and maintaining sustainable, trusted partnerships between the public and private sector. While individual entities are responsible for managing risk to their organization, partnerships improve understanding of threats, vulnerabilities, and consequences through the sharing of indicators and practices and the coordination of policies, response, and recovery activities.

Critical infrastructure partners manage risks based on diverse commitments to community, focus on customer welfare, and corporate governance structures. Risk tolerances will vary from organization to organization, as well as sector to sector, depending on business plans, resources, operating structure, and regulatory environments. Risk tolerances also differ between the private sector and the government based on underlying constraints. As a general rule, private sector organizations can increase their security to meet their risk tolerances and provide for their community of stakeholders, but investment in security and resilience has legitimate limits. In contrast, the government has the mandate to provide for national defense first and foremost. Within these constraints, critical infrastructure security and resilience depends on applying risk management practices of owners and operators and the government to guide efforts.

This section is organized based on the critical infrastructure risk management framework—introduced in the 2006 *NIPP* and updated here – depicted in Figure 4 below. It describes a decision-making process that critical infrastructure partners collaboratively undertake to inform risk management decisions, during both steady-state and crisis operations. Executing a risk management approach is cyclical in nature, and relies on continuous feedback through information-sharing for successful implementation. This framework is not binding and many organizations have risk management processes that have proved effective and should be maintained. Activities are presented within the general context of the critical infrastructure community, but the specific contributions of various partners are called out where appropriate. To support execution of this framework at the organizational level, a supplement (*Implementing the Critical Infrastructure Risk Management Framework)* is provided with this document for reference.

Figure 4 - Critical Infrastructure Risk Management Framework



The critical infrastructure risk management framework is designed to provide maximum flexibility for use in all sectors, across different geographic regions, and by various partners. It can be tailored to dissimilar operating models and environments and applies to all threats and hazards. The risk management framework is intended to complement and support the Threat and Hazard Identification and Risk Assessment (THIRA) process as conducted by regional, SLTT, and urban area jurisdictions to establish capability priorities.

The critical infrastructure community shares information throughout the risk management process to document and build upon best practices and lessons learned; this helps to identify and fill gaps in security and resilience efforts. Information sharing is essential to risk communication, which is defined as the exchange of information with the goal of improving risk understanding, affecting risk perception, and/or equipping people or groups to act appropriately in response to an identified risk.[11]

Risk management enables the critical infrastructure community to focus on those threats and hazards that are likely to cause harm, and employ approaches that are designed to prevent or mitigate the effects of those incidents. It also increases security and strengthens resilience by identifying and prioritizing actions to ensure continuity of essential functions and services and support enhanced response and restoration.

Set Infrastructure Goals and Objectives

This *National Plan* establishes a set of broad national goals for critical infrastructure security and resilience. These national goals are supported by objectives and priorities developed at the sector level, which may be articulated within Sector-Specific Plans (SSPs) and serve as targets for collaborative planning among SSAs and their sector partners in government and the private sector.

Related Calls to Action:
-- Establish National Focus through Joint Priority Setting
-- Determine Collective Actions through Joint Planning Efforts

As discussed in Section 2, a set of national multi-year priorities, developed with input from all levels of the partnership, will complement these goals. Such priorities might focus on particular goals or cross-sector issues where attention and resources could be applied within the critical infrastructure community. Critical infrastructure owners and operators, as well as SLTT and regional entities, can identify

[11] DHS Risk Lexicon, U.S. Department of Homeland Security, 2010.

objectives and priorities for critical infrastructure that align to these national priorities, national goals and sector objectives, but are tailored and scaled to their operational and risk environments.

Identify Critical Infrastructure

To manage risk effectively, it is important to identify which systems, assets, and networks are essential to the functioning of critical infrastructure, considering associated dependencies and interdependencies. This aspect of the risk management process should also identify information and communication technologies that facilitate the provision of essential services.

Critical infrastructure partners view criticality differently, based on their unique situations, operating models, and associated risks. The Federal Government identifies and prioritizes nationally significant critical infrastructure based upon national considerations[12]. SLTT governments identify and prioritize critical infrastructure according to their business and operating environments and associated risks. Critical infrastructure owners and operators identify systems, assets, and networks that are critical to their continued operations and delivery of services and functions to customers. Businesses and jurisdictions evaluate what is most critical to their own functioning and prioritize risk management decisions in the context of their operating and sustainment needs. At the sector level, many SSAs collaborate with owners and operators and SLTT entities to develop lists of critical infrastructure that are significant at the national, regional, and local levels.

Related Call to Action
--Analyze Dependencies and Interdependencies

Effective risk management requires an understanding of criticality as well as the associated interdependencies of critical infrastructure. This National Plan identifies certain lifeline functions that are essential to the operation of most critical infrastructure sectors. These lifeline functions include communications, energy, transportation, and water and waste water. Critical infrastructure partners should identify critical functions and resources that impact their businesses and communities. The identification of these lifeline functions can support preparedness planning and capability development.

Assess and Analyze Risks

Critical infrastructure risks can be assessed in terms of:

- Threat -- natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.
- Vulnerability -- physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.
- Consequence -- effect of an event, incident, or occurrence.

[12] The National Critical Infrastructure Prioritization Program (NCIPP), within DHS, is the primary approach for prioritizing critical infrastructure at the national level. This program identifies nationally significant assets, systems, and networks which, if destroyed or disrupted, could cause some combination of significant casualties, major economic losses, and/or widespread and long-term impacts to national well-being and governance. EO 13636 also assigns DHS the requirement to identify infrastructure in which a cyber incident could result in catastrophic consequences.

Risk assessments are conducted by many critical infrastructure partners to inform their own decision making, using a broad range of methodologies. These assessments allow critical infrastructure community leaders to understand the most likely and severe incidents that could affect their operations and communities and use this information to support planning and resource allocation in a coordinated manner. They can also facilitate collaboration.

To assess risk effectively, critical infrastructure partners—including owners and operators, sector councils, and government agencies—need timely, reliable, and actionable information regarding threats, vulnerabilities, and consequences. In order to achieve awareness, the critical infrastructure community requires that non-governmental entities be involved in the development and dissemination of products regarding threats, vulnerabilities, and potential consequences and are able to provide risk information. Partners should understand intelligence and information requirements and conduct joint analysis where appropriate. Critical infrastructure partnerships can bring great value in improving the understanding of risk to both cyber and physical systems and assets. Neither public nor private sector entities can fully understand the risk without this integration of wide-ranging knowledge and analysis.

Related Calls to Action
-- Improve Information Sharing and Apply Knowledge to Enable Risk-informed Decision Making
-- Empower Local and Regional Partnerships to Build Capacity Nationally

These information sharing initiatives exist both at the national and regional level. Information-sharing activities must also appropriately protect privacy and civil liberties through Fair Information Practice Principles[13] and other similar measures. Equally crucial is ensuring adequate protection of sensitive business and security information that could cause serious adverse impacts to private businesses, the economy, and public or private enterprise security through unauthorized disclosure, access, or use. The Federal Government has a statutory responsibility[14] to safeguard critical infrastructure information. DHS and other agencies use the Protected Critical Infrastructure Information (PCII) program and other protocols such as Classified National Security Information, Law Enforcement Sensitive Information, and Federal Security Classification Guidelines. The PCII program, authorized by the Critical Infrastructure Information (CII) Act of 2002, and its implementing regulations (Title 6 of the Code of Federal Regulations Part 29), define both the requirements for submitting CII and those that government agencies must follow for accessing and safeguarding CII.

Implement Risk Management Activities

Activities to manage critical infrastructure risk are prioritized by decision makers based on the criticality of the affected infrastructure, the costs of such activities and the potential for risk reduction. Some risk management activities address multiple aspects of risk, while others are

[13] The FIPPs are a set of eight principles rooted in the tenets of the Privacy Act of 1974. The eight principles are: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. Sections 222 (a)(1) and (a)(2) of the Homeland Security Act of 2002, as amended, authorize the Chief Privacy Officer to assume primary responsibility for DHS privacy policy.
[14] Section 201(d)(12)(a) of the Homeland Security Act requires DHS to ensure that any material received pursuant to this Act is "protected from unauthorized disclosure and handled and used only for the performance of official duties."

more targeted to address specific threats, vulnerabilities, or potential consequences. These activities can be divided into the following approaches to managing risk:

Detect, Deter, Disrupt, and Prepare for Threats.

Examples of how critical infrastructure partners detect, deter, disrupt, and prepare for threats and hazards include:

- Conducting continuous monitoring of cyber systems;
- Employing security protection systems to detect or delay an attack or intrusion;
- Detecting and disrupting domestic and international criminal and terrorist activities that threaten critical infrastructure and related operational activities across the sectors;
- Implementing intrusion detection or intrusion protection systems on sensitive or mission-critical networks to identify and prevent unauthorized access and exploitations;
- Establishing and implementing joint plans and processes for appropriate increases in security and resilience measures, based on hazard warnings and threat reports; and
- Monitoring critical infrastructure facilities and systems targeted for attack (e.g., through local law enforcement and public utilities).

Related Calls to Action
-- Rapidly Identify, Assess, and Respond to Cascading Effects During and Following Incidents
--Promote Infrastructure, Community, and Regional Recovery Following Incidents

Reduce Vulnerabilities

Examples of vulnerability reduction efforts include:

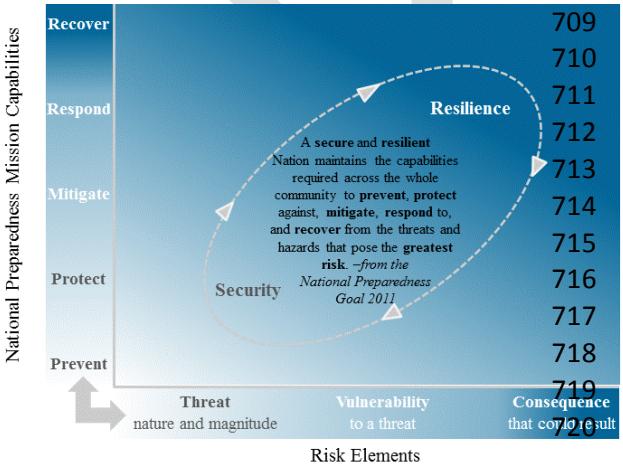
- Building security and resilience into the design and operation of systems, assets and networks;
- Employing siting considerations when locating new infrastructure, such as avoiding floodplains, seismic zones, densely populated areas, and other risk-prone locations;
- Leveraging lessons learned and applying corrective actions from incidents and exercises to enhance protective measures;
- Addressing cyber vulnerabilities through continuous diagnostics and prioritization of high-impact vulnerabilities;
- Developing and conducting training and exercise programs to enhance awareness and understanding of common vulnerabilities and possible mitigation strategies;
- Undertaking R&D efforts to reduce known cyber and physical vulnerabilities that have proved difficult or expensive to address; and
- Establishing and executing business and government emergency action and continuity plans at the local and regional levels to facilitate the continued performance of critical functions during an emergency.

Mitigate Consequences

Critical infrastructure risk management activities that mitigate consequences include:

- Sharing information to support situational awareness and damage assessments of cyber and physical critical infrastructure, including the nature and extent of the threat, cascading effects, and the status of the response;
- Working to restore critical infrastructure operations;
- Ensuring that essential information is backed up on remote servers and that redundant processes are implemented for key functions, reducing the potential consequences of a cybersecurity incident;
- Removing key operational functions from the Internet-connected business network, reducing the likelihood that a cybersecurity incident will result in compromise of essential services;
- Ensuring that incidents affecting cyber systems are fully contained, that asset, system, or network functionality is restored to pre-incident status, and that affected information is available in an uncompromised and secure state;
- Supporting the provision of essential services: for example, emergency power to critical facilities, fuel supplies for emergency responders, and potable water, mobile communications, and food and pharmaceuticals for the affected community;
- Enacting contingency plans to include teleworking, alternate staffing schedules, use of local backup sites, or the movement of operations to other regions;
- Repairing or replacing damaged infrastructure with cost-effective designs that are more secure and resilient;
- Utilizing and ensuring the reliability of emergency communications capabilities;
- Recognizing and accounting for interdependencies in response and recovery/restoration plans; and
- Contributing to the development and execution of private sector, SLTT, and regional priorities for both near- and long-term recovery.

The activities listed above display a sample of risk management activities that are being undertaken to support the overall achievement of security and resilience whether at an organizational, community, sector, or national level.



Based on the National Preparedness System, prevention efforts are most closely associated with efforts to address threats; protection efforts generally address vulnerabilities; and response efforts help minimize consequences, while recovery efforts are key to resilience. Mitigation efforts transcend the entire threat, vulnerability, and consequence spectrum. These five mission areas described in the National Preparedness System provide a useful framework for considering risk management investments.

To execute these missions in advance of or during an incident, the critical infrastructure community should collaborate based on the structures established in the National Prevention Framework, the National Mitigation Framework, the National Response Framework, the National Disaster Recovery Framework, and the interim National Cyber Incident Response Plan (NCIRP). Each of those documents describes structures to enable coordinated activities and information sharing, including with the critical infrastructure community (these include Emergency Support Functions, Recovery Support Functions, and the Cyber Unified Coordination Group). One of the key elements of this *National Plan* is the recognition of the need to integrate the owner and operator community into national preparedness and incident management activities through existing structures. More detail on how that is achieved is available in the associated preparedness doctrine.

An example of how this is achieved is through response efforts. Critical infrastructure-related activities conducted in response to a nationally declared disaster or major incident necessitating Federal assistance are coordinated through the National Response Framework (NRF) organizational structures. The NRF's Critical Infrastructure Support Annex[15] explains how critical infrastructure security and resilience activities are integrated into the NRF and describes policies, roles and responsibilities, incident-related actions, and coordinating structures used to assess, prioritize, secure, and restore critical infrastructure during actual or potential domestic incidents. The Critical Infrastructure Support Annex leverages the partnership structures and information-sharing and risk management processes described in this *National Plan.*

For cyber incident response, critical infrastructure partners at the State, local, tribal, territorial, and regional levels are working to build public-private collaboration, procedures, and capabilities to support an effective and integrated response to cyber incidents. At the national level, the interim NCIRP establishes roles, responsibilities, and actions to prepare for, respond to, and begin to coordinate recovery from cyber incidents. Although steady-state activities and the development of a common operational picture are key components, the NCIRP focuses primarily on building the mechanisms needed to respond to cyber incidents. The NCIRP also recognizes and leverages the role of critical infrastructure partnerships in planning and operations.

In addition to the above threat-, vulnerability-, and consequence-reducing activities, risk reduction can be achieved through critical infrastructure and control system design. Factoring security and resilience measures into design decisions early can facilitate integration of measures to mitigate physical and cyber threats as well as natural and technological hazards at lower cost. Risk analysis, evidence-based design practices, and consideration of costs and benefits can help governments and businesses better invest in measures that increase the security and resilience of both critical infrastructure itself, as well as the broader society that relies on those essential services. There is a particular opportunity to design secure and resilient infrastructure during incident recovery, when both government and the private sector make large investments in repairing, replacing, and strengthening infrastructure and their respective control system environments.

[15] The Critical Infrastructure Support Annex to the National Response Framework, U.S. Department of Homeland Security, 2013.

Measure Effectiveness

The community evaluates achievement of risk management efforts within sectors and at national, State, local, and regional levels by developing aligned metrics for both direct measurement and indirect indicator measurement. In particular, SSAs work through the sector-specific planning process to develop attributes that support the national goals and national priorities as well as other sector-specific priorities. Such measures inform the risk management efforts of partners throughout the critical infrastructure community, and help build a national picture of progress toward the vision of this *National Plan* and the National Preparedness Goal.

Related Calls to Action
-- Evaluate Achievement of Goals
-- Learn and Adapt During and After Exercises and Incidents

At a national level, the goals identified in this *National Plan* articulate broad areas of focus to achieve the *Plan's* vision, and will be complemented by a set of multi-year national priorities. The critical infrastructure community will subsequently identify a high-level outcome associated with each goal and national priority to enable evaluation of its collective success in accomplishing the goals and priorities

This evaluation process functions as an integrated cycle:

- Articulate the vision and national goals;
- Define national priorities;
- Identify a high-level output or outcome associated with each national goal and national priority;
- Collect and share performance data to assess progress in achieving identified outputs and outcomes;
- Evaluate achievement of the national priorities, national goals, and vision;
- Update the national priorities and adapt risk management activities accordingly; and
- Periodically revisit the national goals and vision.

Just as regular evaluation of progress toward the national goals informs the ongoing evolution of security and resilience practices, planned exercises and real-world incidents also provide opportunities for learning and adaptation. For example, fuel shortages after Hurricane Sandy illustrated the challenges in achieving shared situational awareness during large events, as deficiencies in information collection and sharing affected government and private sector partners' ability to coordinate restoration activities. The critical infrastructure and national preparedness communities also conduct exercises on an ongoing basis through the National Exercise Program and other mechanisms to assess and validate the capabilities of organizations, agencies, and jurisdictions. During and after such planned and unplanned operations, partners identify individual and group weaknesses, implement and evaluate corrective actions, and share best practices with the wider critical infrastructure and emergency management communities. Such learning and adaptation inform future plans, activities, technical assistance, training, and education.

6. CALL TO ACTION: FEDERAL STEPS TO ADVANCE THE NATIONAL EFFORT

This Call to Action primarily guides the Federal Government; it can also inform private sector, SLTT, and regional efforts. These activities will be performed in collaboration with critical infrastructure community, recognizing that individual partners have differing priorities and perspectives within sectors, at the State, local, tribal and territorial levels, and among multi-national corporations and small business owners and operators. The following actions are not intended to comprise an exhaustive list, but rather provide strategic direction for national efforts in the coming years:

Build upon Partnership Efforts

1. Set National Focus through Joint Priority Setting
2. Determine Collective Actions through Joint Planning Efforts
3. Empower Local and Regional Partnerships to Build Capacity Nationally
4. Leverage Incentives to Advance Security and Resilience

Innovate in Managing Risk

5. Enable Risk-Informed Decision-Making through Enhanced Situational Awareness
6. Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects
7. Rapidly Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents
8. Promote Infrastructure, Community, and Regional Recovery Following Incidents
9. Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education
10. Improve Critical Infrastructure Security and Resilience by advancing Research and Development Solutions

Focus on Outcomes

11. Evaluate Achievement of Goals
12. Learn and Adapt During and After Exercises and Incidents

These actions will inform and guide efforts identified via the priority-setting and joint planning processes described below.

Build upon Partnership Efforts

Call to Action #1: Set National Focus through Joint Priority Setting

To guide national efforts and inform decisions, the national council structures will jointly set multi-year priorities and review them annually with input from all levels of the critical infrastructure community. Development of the priorities will take into account risks facing the Nation based on the Strategic National Risk Assessment, risk assessments by critical infrastructure partners, and State and regional THIRAs. Annual critical infrastructure and

preparedness reporting will also inform the national priorities through assessment of capability gaps.

- Jointly establish a set of national critical infrastructure security and resilience priorities to support Federal resource allocation and planning and evaluation at all levels in the national partnership.
- Review and validate the national priorities on an annual basis, and update them on a regular cycle timed to inform Federal budget development and SLTT grant programs.

Call to Action #2: Determine Collective Actions through Joint Planning Efforts

Planning activities within the critical infrastructure community should reflect this *National Plan* and the joint priorities established from Call to Action 1. In particular, activities should focus on building SLTT and regional capacity and increasing coordination with the emergency management community.

- All sectors will update their SSPs to support this *National Plan*, and again every four years thereafter, based on guidance developed by DHS in collaboration with the SSAs and cross-sector councils.
    - SSPs will reflect joint priorities
    - SSPs will address sector reliance on critical lifeline functions and include strategies to mitigate consequences from the loss of those functions, including potential cascading effects.
    - SSPs will describe approaches to integrating critical infrastructure and national preparedness efforts, and in particular transitioning from steady state to incident response and recovery via the National Response Framework's Emergency Support Functions (ESFs) and National Disaster Recovery Framework's Recovery Support Functions (RSFs).
    - SSPs will describe current and planned cybersecurity protective efforts, including but not limited to, cybersecurity information sharing initiatives, programmatic activities, risk assessments, exercises, incident response and recovery efforts, and any metrics.
    - SSPs will guide development of appropriate metrics and targets to measure progress toward the national goals and national priorities as well as other sector-specific priorities.
- As appropriate, State, local, tribal, territorial, and regional entities can develop supporting plans to this *National Plan* and the updated SSPs, whether cross-sector or by individual sector, that articulate shared priorities and activities at those levels. The SLTTGCC will collaborate with partners to provide guidance for such plans.
- Release an updated National Cyber Incident Response Plan (NCIRP).

Call to Action #3: Empower Local and Regional Partnerships to Build Capacity Nationally

The local nature of most incidents makes local and regional collaboration essential to integrating critical infrastructure security and resilience and national preparedness activities nationally. Local and regional partnerships contribute significantly to national efforts by increasing the reach of the national partnership, demonstrating its value, and advancing the national goals

- Identify existing local and regional partnerships addressing critical infrastructure security and resilience, their focus and alignment with national partnership structures, and how to engage with them.
- Expand a national network of new and existing regional partnerships and coalitions to complement and enhance the national-level focus on sectors, while remaining cognizant of varying legal structures in different jurisdictions and organizations.
- Adapt the THIRA process to better integrate human, physical, and cyber elements of critical infrastructure risk and resilience. This would enable coordinated planning, resource allocation, and evaluation of progress by State and local governments and local infrastructure owners and operators based on integrated plans for community and infrastructure preparedness, security, and resilience.
- Federal agencies responsible for implementing PPD-8 and PPD-21 develop (in collaboration with State, metropolitan areas and regional coalitions) and advance a joint set of regional projects demonstrating the integrated application of critical infrastructure and national preparedness risk and resilience analysis, planning, and risk management activities.

Call to Action #4: Leverage Incentives to Advance Security and Resilience

The government and the private sector have a shared interest in ensuring the viability of critical infrastructure and the provision of essential services, under all conditions. Critical infrastructure owners and operators are often the greatest beneficiaries of investing in their own security and resilience, and are influenced by a social responsibility to adopt such practices. However, the private sector may be justifiably concerned about the return on security and resilience investments that may not yield immediately measureable benefits. Effective incentives can help justify the costs of improved security and resilience by balancing the short-term costs of additional investment with similarly near-term benefits. Market-based incentives can promote significant changes in business practices and encourage the development of markets such as insurance for cyber, chemical, biological, or radiological risks. Additionally, States and localities can explore offering their own incentives to encourage investment in security and resilience measures.

- Continue to analyze and, where appropriate, implement incentives
- Support research and data gathering to quantify the potential costs imposed by a lack of critical infrastructure security and resilience, including cyber insecurity.
- Establish innovation challenge programs to incentivize new solutions to strengthen infrastructure security and resilience during infrastructure planning, design and redesign phases, including technological, engineering, and process improvements.

Innovate in Managing Risk

Call to Action #5: Enable Risk-Informed Decision Making through Enhanced Situational Awareness

To ensure that situational awareness capabilities keep pace with a dynamic and evolving risk environment, the critical infrastructure community must continue to improve practices for sharing information and applying the knowledge gained through changes in policy, process, and

culture. The community can promote a culture of "need to share" and "responsibility to provide" across all levels and sectors, recognizing that critical infrastructure owners and operators and SLTT governments are crucial consumers *and* providers of risk information. This culture is built on a shared understanding of national efforts toward greater critical infrastructure security and resilience.

Accordingly, the Federal Government will consult with State and local governments and owners and operators to ensure that intelligence analyses meet their needs, and exercise consistent means for disseminating intelligence and information security products. It will also continue to enhance the ability of the NICC, NCCIC, and other Federal information sharing resources to produce and share a cross-sector, near real-time situational awareness picture while protecting sensitive data (for more, see the supplement "How to Connect to the NICC and NCCIC"). In addition, the Federal Government will leverage "tearline" and "shareline"[16] policies and procedures to facilitate sharing of actionable portions of otherwise classified or restricted unclassified reports with private sector and SLTT partners. Likewise, State and local governments can improve information sharing between State and local fusion centers and State homeland security advisors. State and local governments and regional partnerships can promote greater use of State and local fusion centers within their respective jurisdictions and regions to inform threat identification, risk assessment, and priority development. Owners and operators can support improvements by giving government intelligence analysts ongoing feedback on the dissemination and application of their information products and sharing information with Federal and SLTT governments.

- Undertake a partnership-wide review of impediments to information sharing to support efforts to address those challenges and develop best practices. Analyze legal considerations, the classification or sensitive nature of certain information, laws and policies that govern information dissemination, and the need to build trust among partners.
- Building upon the functional relationship descriptions developed as part of PPD-21, further analyze functional relationships within and across the Federal Government (focused on critical infrastructure security and resilience) to identify overlaps, inefficiencies, and gaps, and recommend changes to enhance situational awareness and risk-informed decision making.
- Develop streamlined, standardized processes to promote integration and coordination of information sharing via jointly developed doctrine and supporting standard operating procedures (SOPs).
- Develop interoperability standards, as suggested in PPD 21, to enable more efficient information exchange through defined data standards and requirements, including developing: (1) the foundation of an information-sharing environment that has common data requirements and information flow and exchange across entities, and (2) sector-specific critical infrastructure requirements (i.e., critical reporting criteria) to allow for

[16] "Tearlines" are portions of an intelligence report or product that provide the substance of a more classified or controlled report without identifying sources, methods, or other operational information. Tearlines release classified intelligence information with less restrictive dissemination controls, and, when possible, at a lower classification; "shareline" refers to an unclassified and less restrictive portion or excerpt of a report or other information source that provides the substance of a dissemination-controlled report.

improved information flow and reporting and to produce more complete and timely situational awareness.

Call to Action #6: Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects

Greater analysis of dependencies and interdependencies at international, national, regional, and local levels can inform planning and facilitate prioritization of resources to ensure the continuity of critical services and mitigate the cascading impacts of incidents that do occur.

- Mature the capability to identify and categorize cross-sector physical and cyber dependencies and interdependencies over different time frames at international, national, regional, and local levels. Focus on the lifeline functions and the resilience of global supply chains during potentially high-consequence incidents given their importance to public health, welfare, and economic activity.
- Continue to evolve the Cyber Dependent Infrastructure Information (CDII) approach under Executive Order 13636 to consider the potential risks from dependency on information and communications technology and inform preparedness planning and capability development.

Call to Action #7: Rapidly Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents

Critical infrastructure and emergency response planning and exercises, as well as real-world events, underscore the need to prepare for cascading effects during incidents that could potentially magnify consequences. While understanding of dependencies and interdependencies is a key aspect of ongoing risk management efforts and preparedness planning, it is not possible to foresee all the interactions that may emerge within complex systems of systems during an incident. Therefore, the critical infrastructure community can significantly advance the Nation's preparedness for all hazard incidents by developing the capability to rapidly identify, assess, and respond to cascading effects beginning with the lifeline functions during and following incidents.

- Enhance the capability to rapidly identify and assess cascading effects involving the lifeline functions and contribute to identifying infrastructure priorities – both known and emerging – during response and recovery efforts.
- Enhance the capacity of critical infrastructure partners to work through incident management structures such as the Emergency Support Functions to mitigate the consequences of disruptions to the lifeline functions.

Call to Action #8: Promote Infrastructure, Community, and Regional Recovery Following Incidents

Recent incidents highlight the need for long-term recovery capabilities to enhance the security and resilience of infrastructure, communities, and regions during rebuilding. Developing such capabilities will require critical infrastructure partners to leverage existing trust relationships and engage a spectrum of whole community partners active in recovery, including citizens, non-profits, business leaders, and government representatives not usually involved in infrastructure or security discussions.

- Leverage Federal field staff (including Protective Security Advisors) – and encourage States and localities – to promote consideration of critical infrastructure challenges in pre-incident recovery planning, post-incident damage assessments, and development of recovery strategies.
- Support initiatives to enhance and replace infrastructure providing lifeline functions during recovery.

Call to Action #9: Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education

To continue to execute and sustain the risk management activities described in this section and prepare organizations and professionals to meet future challenges, the critical infrastructure community must continue to innovate in its development and delivery of technical assistance, training, and education programs and its assessment of their effectiveness.

- Capture, report, and prioritize the technical assistance, training, and education needs of the various partners within the critical infrastructure community.
- Examine current Federal technical assistance, training, and education programs to ensure that they support the national priorities and the risk management activities described in this *National Plan* in order to advance progress toward the national goals.
- Increase coordination of technical assistance efforts – particularly within DHS among the SSAs – and leverage a wider network of partners to deliver training and education programs in order to better serve recipients and reach a wider audience while conserving resources.
- Partner with academia to evolve critical infrastructure curriculum to develop critical infrastructure professionals, including executives and managers, trained to manage the benefits and inherent vulnerabilities that information and communications technology introduces in critical infrastructure assets, systems, and networks.

Call to Action #10: Improve Critical Infrastructure Security and Resilience by advancing Research and Development Solutions

PPD-21 directs the Federal Government to provide a research and development (R&D) plan that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide research and development requirements and investments. The *National Critical Infrastructure Security and Resilience R&D Plan* will be reissued every four years after its initial delivery, with interim updates as needed. Its focus will include:

- Promoting research and development to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;
- Enhancing modeling capabilities to determine potential impacts on critical infrastructure of an incident or threat scenario, as well as cascading effects on other sectors;
- Facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen all-hazards security and resilience; and

- Prioritizing efforts to support the strategic guidance issued by the Secretary of Homeland Security.

To increase infrastructure security and resilience, research and development requires coordination to address analytic and policy capability gaps, improve risk management capabilities for owner-operators, and execute and transition R&D into operational use. Priorities may emerge from the R&D plans of the 16 sectors, both from commonly embraced requirements, and from discrete requirements that provide the greatest potential return. *The National Critical Infrastructure Security and Resilience R&D Plan* will use sector-specific research and development planning documents that address R&D needs and priorities from the perspective of their sectors.

Focus on Outcomes

Call to Action #11: Evaluate Achievement of Goals

While much of the groundwork for the integrated evaluation cycle described in Section 5 already exists, wider and more consistent participation by critical infrastructure partners is necessary to accurately understand progress and facilitate adaptive decision making.

- Jointly identify a high-level output or outcome associated with each national goal and national priority to facilitate evaluation of progress toward the goals and priorities.
- Develop the Critical Infrastructure National Annual Report and National Preparedness Report annually though standardized data calls to SSAs to gather valid, complete, consistent, accurate, and timely performance data to build a national picture of progress toward this *National Plan's* national goals and vision and the National Preparedness Goal. Incorporate performance data from industry, SLTT, and regional entities to reflect progress throughout the critical infrastructure community at all levels.

Call to Action #12: Learn and Adapt During and After Exercises and Incidents

Given the evolving nature of threats, hazards, and resilience, the national aspiration of secure and resilient critical infrastructure is achievable only through the collective efforts of numerous partners grounded in continuous learning and adaptation to changing environments. The critical infrastructure community can better realize the opportunities for learning and adaptation during and after exercises and incidents through more collaborative exercise design, coordinated lessons learned and corrective action processes, and streamlined sharing of best practices.

- Develop and conduct exercises through participatory processes to suit diverse needs and purposes.
    - Promote broad participation and coordination among government and interested private sector partners – including the R&D community – in exercise design, conduct, and evaluation to reflect the perspectives of all partners and maximize the value for future planning and operations.
    - Develop exercises at multiple levels and in various formats to suit national, regional, and SLTT needs.
- Design exercises to reflect lessons learned and test corrective actions from previous exercises and incidents, address both physical and cyber threats to and vulnerabilities in

critical infrastructure, and evaluate the transition from steady state to incident response and recovery efforts.

- Share lessons learned and corrective actions from exercises and incidents and rapidly incorporate them into technical assistance, training, and education to improve future prevention, protection, mitigation, response, and recovery actions.

The actions listed in this section are not intended to be exhaustive, but rather to direct the Federal Government and inform the critical infrastructure community to advance the national effort toward security and resilience. Through coordinated and flexible implementation by Federal departments and agencies – as well as SLTT, regional, and private sector partners as appropriate given their unique risk management perspectives – these actions will enable continuous improve of security and resilience efforts to address both familiar and novel challenges.

Glossary of Terms

Many of the definitions in this Glossary are derived from language enacted in Federal laws and/or included in national plans, including the Homeland Security Act of 2002, the USA PATRIOT Act of 2001, the 2009 NIPP, Presidential Policy Directive (PPD) 8, *National Preparedness*, and PPD-21, *Critical Infrastructure Security and Resilience*. Additional definitions come from the DHS Lexicon. The source for each entry below follows each definition.

All Hazards. The term "all hazards" means a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure. (Source: PPD-21, 2013)

Asset. Person, structure, facility, information, material, or process that has value. (Source: DHS Lexicon, 2010)

Business Continuity. Those activities performed by an organization to ensure that during and after a disaster the organization's essential functions are maintained uninterrupted, or are resumed with minimal disruption. (Source: Derived from the 2009 NIPP)

Consequence. The effect of an event, incident, or occurrence, including the number of deaths, injuries and other human health impacts along with economic impacts both direct and indirect along with other negative outcomes to society. (Source: Derived from DHS Lexicon, 2010)

Control Systems. Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of types of control systems include SCADA systems, Process Control Systems, and Distributed Control Systems. (Source: 2009 NIPP)

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: section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e))

Critical Infrastructure Community. Critical infrastructure owners and operators, both public and private; Federal departments and agencies; regional entities; State, local, tribal, and territorial (SLTT) governments; and other organizations from the private and nonprofit sectors with a role in securing and strengthening the resilience of the Nation's critical infrastructure.

Critical Infrastructure Cross-Sector Council. Council comprises the leadership of the SCCs. The private sector cross-sector council coordinates cross-sector issues, initiatives, and interdependencies to support critical infrastructure security and resilience.

Critical Infrastructure Information (CII). Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems. CII consists of records and information concerning any of the following:

- Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer- based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law; harms the interstate commerce of the United States; or threatens public health or safety.
- The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit.
- Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, insurance, or continuity, to the extent that it is related to such interference, compromise, or incapacitation. (Source: 2009 NIPP)

Critical Infrastructure Owners and Operators. Those entities responsible for day-to-day operation and investment in a particular asset or system. (Source: 2009 NIPP)

Critical Infrastructure Partner. Those Federal, State, local, tribal, or territorial governmental entities, public and private sector owners and operators and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share in the responsibility for securing and strengthening the resilience of the Nation's critical infrastructure. (Source: 2009 NIPP)

Critical Infrastructure Partnership Advisory Council (CIPAC). The 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: PPD-21, 2013)

Critical Infrastructure Risk Management Framework. A planning and decision-making framework that outlines the process for setting goals and objectives; identifying critical infrastructure; assessing risks; implementing risk management activities; and measuring effectiveness to inform continuous improvement in critical infrastructure security and resilience. (Source: Derived from the 2009 NIPP)

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)

Cyber Unified Coordination Group (UCG). The Cyber UCG is comprised of senior and staff level representatives from federal departments and agencies, state and local governments, and private sector critical infrastructure stakeholders. (Source: NIST)

Cyber System. Any combination of facilities, equipment, personnel, procedures, and communications integrated to provides cyber services. Examples include business systems, control systems, and access control systems. (Source: 2009 NIPP)

Dependency. The one-directional reliance of an asset, system, network, or collection thereof—within or across sectors—on an input, interaction, or other requirement from other sources in order to function properly. (Source: 2009 NIPP)

EO 13636. Executive Order (EO) 13636,[17] *Improving Critical Infrastructure Cybersecurity* (February 2013). EO 13636 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. (Source: EO 13636, 2013)

Emergency Support Functions (ESF). The Federal ESFs are the primary, but not exclusive, Federal coordinating structures for building, sustaining, and delivering the response core capabilities. The ESFs are vital structures for responding to Stafford Act incidents; however, they may also be used for other incidents. (Source: *National Response Framework*)

Federal Departments and Agencies. Any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5). (Source: PPD-21, 2013)

Function. Service, process, capability, or operation performed by an asset, system, network, or organization. (Source: DHS Lexicon, 2010)

Fusion Center. A focal point within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government and State, local, tribal, territorial, and private sector partners. (Source: DHS Lexicon, 2010)

Government Coordinating Council. The government counterpart to the Sector Coordinating Council for each sector, established to enable interagency and intergovernmental coordination. The GCC comprises representatives across various levels of government (Federal, State, local, tribal, and territorial) as appropriate to the risk and operational landscape of each sector. (Source: 2009 NIPP)

Hazard. Natural or manmade source or cause of harm or difficulty. (Source: DHS Lexicon, 2010)

Incident. An occurrence, caused by either human action or natural phenomenon that may cause harm and require action. Incidents can include major disasters, emergencies, terrorist attacks, terrorist threats, wild and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, cyber attacks, cyber failure/accident, and other occurrences requiring an emergency response. (Source: Derived from DHS Lexicon, 2010)

Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capa-

[17] EO 13636 can be found at: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

bilities 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)

Interdependency. Mutually reliant relationship between entities (objects, individuals, or groups). The degree of interdependency does not need to be equal in both directions. (Source: DHS Lexicon, 2010)

Joint Terrorism Task Forces (JTTFs). FBI-led multi-jurisdictional task forces of highly trained and locally based investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies, including State and local law enforcement agencies, focused primarily on terrorism-related issues and investigations.

Mitigation. Those capabilities necessary to reduce loss of life and property by lessening the impact of disasters. (Source: PPD-8, 2011)

National Cyber Investigative Joint Task Force (NCIJTF). The multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from federal agencies, including DHS, and from State, local, and international law enforcement partners. (Source: FBI Web site, www.fbi.gov)

National Cybersecurity and Communications Integration Center (NCCIC). The national cyber critical infrastructure center, as designated by the Secretary of Homeland Security, secures Federal civilian agencies in cyberspace; provides support and expertise to private sector partners and State, local, tribal, and territorial entities; coordinates with international partners; and coordinates the Federal Government mitigation and recovery efforts for significant cyber and communications incidents. (Source: DHS Web site, www.dhs.gov)

National Infrastructure Coordinating Center (NICC). The national physical infrastructure center, as designated by the Secretary of Homeland Security, coordinates a national network dedicated to the security and resilience of critical infrastructure of the United States by providing 24/7 situational awareness through information sharing, and fostering a unity of effort. (Source: DHS Web site, www.dhs.gov)

National Operations Center (NOC). A DHS 24/7 operations center responsible for providing real-time situational awareness and monitoring of the homeland, coordinating incidents and response activities and, in conjunction with the Office of Intelligence and Analysis, issuing advisories and bulletins concerning threats to homeland security, as well as specific protective measures. (Source: DHS Web site, www.dhs.gov)

National Preparedness. The actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. (Source: PPD-8, 2011)

Network. A group of components that share information or interact with each other in order to perform a function. (Source: 2009 NIPP)

Partnerships. Within the context of this plan, it is defined as close cooperation between parties having common interests in achieving a shared vision.

PPD-8. Presidential Policy Directive 8 (PPD-8) *National Preparedness* (March 2011). PPD-8 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. PPD-8 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)

PPD-21. Presidential Policy Directive 21[18] (PPD-21), *Critical Infrastructure Security and Resilience* (February 2013). This directive 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)

Prevention. As defined in PPD-8, prevention includes those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. (Source: PPD-8, 2011).

Prioritization. In the context of critical infrastructure security and resilience, prioritization is the process of using risk assessment results to identify where risk reduction or mitigation efforts are most needed and subsequently determine which security and resilience activities should be implemented to have the greatest effect. (Source: 2009 NIPP)

Protected Critical Infrastructure Information (PCII). PCII refers to all critical infrastructure information, including categorical inclusion PCII, that has undergone the validation process and that the PCII Program Office has determined qualifies for protection under the CII Act. 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. (Source: 2009 NIPP)

Protection. Those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. (Source: PPD-8, 2011)

Recovery. Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources. (Source: PPD-8, 2011)

Recovery Support Functions. The Recovery Support Functions (RSFs) comprise the *National Disaster Recovery Framework's (NDRF's)* coordinating structure for key functional areas of assistance. Their purpose is to support local governments by facilitating problem solving, improving access to resources and by fostering coordination among State and Federal agencies, nongovernmental partners and stakeholders. (Source: FEMA.gov)

Regional. For purposes of this national plan, regional refers to entities and interests spanning geographic areas ranging from large multi-State areas to metropolitan areas and varying by organizational structure and key initiatives, yet fostering engagement and collaboration between

[18] PPD-21 can be found at: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

critical infrastructure owners and operators, government, and other key stakeholders within the given location. (Source: RC3 Regional Partnership Study Report, 2011)

Regional Consortium Coordinating Council (RC3). RC3 comprises regional groups and coalitions around the country engaged in various initiatives to advance critical infrastructure security and resilience in the public and private sectors.

Resilience. The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (Source: PPD-21, 2013)

Response. Those capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. (Source: PPD-8, 2011)

Risk. The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. (Source: DHS Lexicon, 2010)

Risk-Informed Decision Making. The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other relevant factors. (Source: 2009 NIPP)

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The NIPP addresses 16 critical infrastructure sectors, as identified in PPD-21. (Source: 2009 NIPP)

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. SCCs serve as the government's principal point of entry into each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. (Source: 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 (SSPs). Planning documents that complement and tailor application of the Critical Infrastructure National 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: Derived from the 2009 NIPP)

Secure / Security. Reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters. (Source: PPD-21, 2013)

Steady State. In the context of critical infrastructure security and resilience, steady state is the posture for routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents. (Source: DHS Lexicon, 2010)

System. Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose. (Source: DHS Lexicon, 2010)

Terrorism. Premeditated threat or act of violence against noncombatant persons, property, and

environmental or economic targets to induce fear, intimidate, coerce, or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives. (Source: DHS Lexicon, 2010)

Threat. A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. (Source: DHS Lexicon, 2010)

Value Proposition. A statement that outlines the national and homeland security interest in protecting the Nation's critical infrastructure and articulates the benefits gained by all critical infrastructure partners through the risk management framework and public-private partnership described in the Critical Infrastructure National Plan. (Source: 2009 NIPP)

Vulnerability. A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. (Source: DHS Lexicon, 2010)

Appendix A. The National Partnership Structure

The collaboration between private sector owners and operators and their counterpart government agencies was first established through the NIPP and further refined by PPD-21, which organized the Nation's critical infrastructure into 16 sectors, defined Sector-Specific Agencies (SSAs) for each of the sectors, and established the requirement for partnerships of the Federal Government, critical infrastructure owners and operators, and State, local, tribal, and territorial (SLTT) government entities. This sector and cross-sector partnership council structure – consisting of Sector Coordinating Councils (SCCs), Governmental Coordinating Councils (GCCs), SSAs, and cross-sector councils – brings together partners from Federal, SLTT governments, regional entities, the private sector, and non-governmental organizations to collaborate on critical infrastructure security and resilience programs and approaches, and to achieve national goals and objectives. These councils provide the primary organizational structure for coordinating critical infrastructure security and resilience efforts and activities within and across the 16 sectors.

Sector Coordinating Structures

The public-private coordination for critical infrastructure security and resilience is built through the joint efforts of the three components of the critical infrastructure sector partnership--SCCs, GCCs, and SSAs. Each of these components serves interests within their own constituencies in addition to providing an interface with its partners. The unique features of these elements of the partnership are presented below.

Sector Coordinating Councils – The SCCs are self-forming, self-organizing, and self-governing councils that enable owners and operators, their trade associations, vendors, and others to interact on a wide range of sector-specific strategies, policies, activities, and issues. The SCCs serve as principal sector policy coordination and planning entities to collaborate with SSAs and related GCCs to address the entire range of critical infrastructure security and resilience activities and issues for that sector. As such, they serve as a voice for the sector and represent the government's principal entry into the sector. In addition, the SCCs are encouraged to participate in efforts to develop voluntary consensus standards to ensure that sector perspectives are included.

Other primary functions of an SCC may include:

- Serve as a strategic communications and coordination mechanism between owners, operators, and suppliers, and, as appropriate, with the government during emerging threats or response and recovery operations, as determined by the sector;
- Identify, implement, and support appropriate information-sharing capabilities and mechanisms in sectors where no information sharing structure exists;
- Facilitate representation throughout the sector;
- Participate in planning efforts related to the revision of the National Plan and development and revision of Sector-Specific Plans (SSPs); review the annual submission to DHS on sector activities;
- Facilitate inclusive organization and coordination of the sector's policy development

regarding critical infrastructure security and resilience planning and preparedness, exercises and training, public awareness, and associated implementation activities and requirements;

- Identify, develop, and share information with the sector, both public and private sector members, concerning effective cybersecurity practices, such as cybersecurity working groups, risk assessments, strategies, and plans;
- Understand and communicate requirements of the sector for government support; and
- Provide input to the government on sector R&D efforts and requirements.

Government Coordinating Councils – The GCCs enable interagency, intergovernmental, and cross-jurisdictional coordination within and across sectors. The GCCs comprise representatives from across various levels of government (Federal and SLTT), as appropriate to the operating landscape of each individual sector. Each GCC is chaired by a representative from the designated SSA with responsibility for ensuring appropriate representation on the council and providing cross-sector coordination with SLTT governments. For DHS GCC, the Assistant Secretary for Infrastructure Protection co-chairs the Council. The GCC coordinates strategies, activities, policies, and communications across governmental entities within each sector. Reaching across the partnership, the GCC works to coordinate with and support the efforts of the SCC.

Other primary functions of a GCC include the following:

- Provide interagency strategic communications and coordination at the sector level through partnership with DHS, the SSA, and other supporting agencies across various levels of government;
- Participate in planning efforts related to the revision of the NIPP and the development and revision of SSPs;
- Coordinate strategic communications and discussion and resolution of issues among government entities within the sector;
- Promote adoption of physical and cyber risk management process across the sector;
- Enhance government information sharing across the sector and promote multi-channel public-private information sharing;
- Identify and support the information-sharing capabilities and mechanisms that are most appropriate for the SLTT governments; and
- Coordinate with and support the efforts of the SCC to plan, implement, and execute the Nation's critical infrastructure security and resilience mission.

Sector-Specific Agencies – Recognizing existing statutory or regulatory authorities of specific Federal departments and agencies, and leveraging existing sector familiarity and relationships, SSAs serve as the Federal interface for the prioritization and coordination of sector-specific security and resilience efforts and carry out incident management responsibilities for their sectors. For sectors subject to Federal or State regulation, the SSA coordinates these activities with the regulator, as appropriate. SSAs promote sector-wide information sharing and support the national program by addressing joint national priorities

and reporting on progress toward achieving security and resilience outcomes. More detail on the specific roles and responsibilities of SSAs is provided in Appendix B.

Cross-Sector and Regional Coordinating Structures

All cross-sector councils participate in planning efforts related to the development of national priorities and related policy and planning documents that guide critical infrastructure security and resilience efforts at the national level, including this *National Plan*. Each of these councils is described below.

Critical Infrastructure Cross-Sector Council – Cross-sector issues and interdependencies are addressed among the SCCs through the Critical Infrastructure Cross-Sector Council, which comprises the leadership of the SCCs. The Council coordinates cross-sector initiatives to support critical infrastructure security and resilience by identifying issues that affect such initiatives and by raising awareness. The primary activities of the Council include:

- Providing senior-level, cross-sector strategic coordination through partnership with DHS and the SSAs;
- Identifying and disseminating critical infrastructure security and resilience best practices across the sectors;
- Identifying areas where cross-sector collaboration could advance national priorities; and
- Coordinating with government at all levels to support efforts to plan and execute the Nation's critical infrastructure security and resilience mission.

Federal Senior Leadership Council (FSLC) – The objective of the FSLC is to facilitate enhanced communication and coordination across the sectors among Federal departments and agencies with a role in implementing initiatives focused on critical infrastructure security and resilience. The council's primary activities include:

- Forging consensus on risk management strategies;
- Evaluating and promoting implementation of risk-informed critical infrastructure security and resilience programs;
- Coordinating strategic issues and issue management resolution among Federal departments and agencies, and State, regional, local, tribal, and territorial partners;
- Advancing collaboration within and across sectors and with the international community;
- Advocating for and tracking execution of the *National Plan* across the Executive Branch;
- Supporting development of resource requests to fulfill the Federal mission;
- Encouraging voluntary adoption of a common risk analysis and decision-support process across all sectors; and
- Evaluating and reporting on the progress of Federal critical infrastructure security and

resilience activities.

State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) – The SLTTGCC serves as a forum to promote the engagement of SLTT partners as active participants in national critical infrastructure security and resilience efforts and to provide an organizational structure to coordinate across jurisdictions on State and local government-level guidance, strategies, and programs. The SLTTGCC:

- Provides senior-level, cross-jurisdictional strategic communications and coordination through partnership with the Federal Government and critical infrastructure owners and operators;
- Coordinates strategic issues and issue management resolution among Federal departments and agencies, and SLTT partners;
- Coordinates with the Federal Government and owners and operators to support efforts to plan, implement, and execute the Nation's critical infrastructure security and resilience mission;
- Provides DHS with information on SLTT-level security and resilience initiatives, activities, and best practices; and
- Cooperates with DHS in establishing test sites for demonstration projects to support innovation.

Regional Consortium Coordinating Council (RC3) – The RC3 provides a framework that supports existing regional groups in their efforts to promote resilience activities in the public and private sectors. Comprised of a variety of regional groups from around the country, the RC3 supports its member organizations with awareness, education, and mentorship on a wide variety of subjects, projects, and initiatives. The RC3 is engaged in various initiatives to advance critical infrastructure security and resilience, vulnerability reduction, and consequence mitigation, including the following:

- Partnering with the Critical Infrastructure Cross-Sector Council and the SLTTGCC to improve information sharing and communication throughout the national partnership and identify ways the three councils can leverage each other's membership and knowledge;
- Hosting webinars to enhance partners' understanding of the roles of the RC3, the Critical Infrastructure Cross-Sector Council, and the SLTTGCC in critical infrastructure security and resilience;
- Conducting regional catastrophic event response and recovery exercises in conjunction with existing regional workshops;
- Identifying best practices and standards for the use of social media tools in critical infrastructure security and resilience;
- Developing a communication and collaboration strategy that embraces social technology and employs controls and practices that are efficient, effective, and commensurate with the emerging risk environment; and

- Aiding in the development and coordination of State and local Critical Infrastructure Asset Registries.

Information Sharing and Analysis Organizations – Several private sector information sharing and analysis organizations have been established over the last decade. Information Sharing and Analysis Centers (ISACs) are examples of successful information sharing organizations.

ISACs. ISACs serve as operational and dissemination arms for many sectors and sub-sectors, and facilitate sharing of information between government and the private sector. ISACs work closely with SCCs in the sectors where they are recognized. ISACs are designed to provide in-depth sector analysis and help coordinate sector information sharing efforts during incidents. Government agencies may also rely on ISACs for situational awareness and to enhance their ability to provide timely, actionable data to targeted entities. As of the publication of this *National Plan*, the National Council of ISACs serves as the coordinating body for ISACs and provides senior-level, cross-sector operational coordination by partnering with the other cross-sector councils, DHS, and the SSAs.

Critical Infrastructure Partnership Decision Making

The Critical Infrastructure Partnership Advisory Council (CIPAC) [19] was established by the Secretary of Homeland Security in 2006 as a mechanism to directly support the sectors' interest to jointly engage in critical infrastructure discussions and to participate in a broad spectrum of activities. Specifically, CIPAC forums serve an advisory role by supporting deliberations on critical infrastructure issues that are needed to arrive at a consensus position or when making formal recommendations to the Federal Government. Discussions and activities undertaken after invoking CIPAC include the following:

- Plan, coordinate, and exchange information on sector-specific or cross-sector issues;
- Conduct operational activities related to critical infrastructure security and resilience, both in steady state and during incident response;
- Contribute to the development and implementation of national policies and plans, including this *National Plan* and the SSPs; and
- Submit consensus recommendations to the Federal Government related to critical infrastructure programs, tools, and capabilities.

CIPAC members are representatives of their respective GCCs and SCCs. CIPAC-covered groups are convened with representatives of GCCs and SCCs when there is a need to seek consensus on an issue. CIPAC-covered activities convene GCC and SCC representatives when there is need to seek consensus on an issue. As such, CIPAC may be used at the sector, cross-sector, or working group levels, depending on the topic and deliberation purpose. Meetings, forums, and other CIPAC activities are attended by government and private sector representatives, and often include invited subject matter experts who present on a specific topic.

Whereas the CIPAC statutory framework provides a common legal framework for collaboration on critical infrastructure issues at the national level, there is no such legal framework to enable

[19] Critical Infrastructure Partnership Advisory Council. http://www.dhs.gov/critical-infrastructure-partnership-advisory-council

coordinated activities at the State, regional, and local levels. Multiple and varied state sunshine and antitrust laws vastly complicate the coordination and collaboration by network operators and other entities at the State, regional and local levels. Without a common legal framework, coordination at these levels is fraught with difficulties.

Information Sharing for Critical Infrastructure Security and Resilience

In addition to information disseminated by SSAs and other national partnership mechanisms, there are information sharing and analysis organizations that address national issues but also serve day-to-day operational roles at the SLTT levels and work with public and private owners and operators. These include the National Infrastructure Coordinating Center (NICC), and the National Cybersecurity and Communications Integration Center (NCCIC), the National Operations Center (NOC), and the National Cyber Investigative Joint Task Force (NCIJTF).

NICC and NCCIC. PPD-21 states that **"**There shall be two national critical infrastructure centers operated by DHS – one for physical infrastructure [NICC] and another for cyber infrastructure [NCCIC]. They shall function in an integrated manner and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect the physical and cyber aspects of critical infrastructure." The NICC serves as a clearinghouse of information to receive and synthesize critical infrastructure information and provide that information back to decision-makers at all levels to enable rapid, informed decisions in steady state, heightened alert and during incident response. The NCCIC is a round-the-clock information sharing, analysis, and incident response center where government, private sector, and international partners share information and collaborate on response and mitigation activities to reduce the impact of significant incidents, enhance partners' security posture, and develop and issue alerts and warnings while creating strategic and tactical plans to combat future malicious activity. An integrated analysis component, also required by PPD-21, works in coordination with both centers to contextualize and facilitate greater understanding of the information streams flowing through the two centers.

These centers, along with an integrated analysis function, build situational awareness across critical infrastructure sectors based on partner input and provide information with greater depth, breadth, and context than the individual pieces from any individual partner or sector. A guide on how to work with and use the NICC and NCCIC is available as a supplement to this plan.

NOC. The NOC is the principal operations center for DHS, consisting of a NOC Watch, Intelligence Watch and Warning, FEMA's National Watch Center and National Response Coordination Center, and the NICC. It collects and fuses information from more than 35 Federal, State, territorial, tribal, local, and private sector entities. The NOC provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities, and issues advisories and bulletins concerning threats to homeland security, as well as specific protective measures. The NOC–which operates 24 hours a day, 365 days a year–coordinates information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents.

NCIJTF. The Federal Bureau of Investigation is responsible for the operation of the NCIJTF, the interagency cyber center with primary responsibility for developing and sharing information related to cyber threat investigations and for coordinating and

integrating associated operational activities to counter cyber threats, including threats to critical infrastructure. The NCIJTF is an alliance of peer agencies with complementary missions to protect national cyber interests. Representatives from participating Federal agencies, including DHS, and from State, local, and international law enforcement partners, have access to comprehensive views of cyber threat situations, while working together in a collaborative environment.

Collaborative Approaches across the Critical Infrastructure Community

The partnership approach is designed to encourage participation from across the community and allow individual owners and operators of critical infrastructure and other stakeholders across the country to participate. It also is intended to promote consistency of process to enable efficient collaboration between disparate parts of the critical infrastructure community. This does not imply that the sector and cross-sector partnership structure should be replicated at the regional, State, and local levels, however its proven utility can serve as a model and bring value at various levels.

Regional partnerships have brought together diverse interests across State boundaries, metropolitan areas, infrastructure sectors, and operational interests to build organizations to address shared concerns. Collaborating at the regional level requires flexibility to engage other entities that play a role in critical infrastructure security and resilience such as the Federal Bureau of Investigation's InfraGard chapters, Weapons of Mass Destruction Coordinators, Field Intelligence Groups, and Joint Terrorism Task Forces. The FBI JTTFs are comprised of regional, State, and local law enforcement and should be considered the "intake" centers for critical infrastructure partners to report suspicious activity that may potentially constitute a nexus to terrorism. The FBI shares threat information with its partners though its JTTFs and other field components. Other collaboration is conducted through the Domestic Security Alliance Council,[20] and the National Network of State Fusion Centers, which function at the State and major urban area fusion centers level.

Fusion centers help owners and operators and government partners stay informed of emerging threats and vulnerabilities. State and local government representatives (e.g., emergency management, public health, public safety) have daily interaction with fusion centers' threat intake, analysis, and sharing functions. Homeland Security Advisors, Protective Security Advisors, and Cybersecurity Advisors also interface with the fusion centers.

The State component of the critical infrastructure partnership extends beyond the SLTTGCC to include State coalitions and operational partnerships and, where possible, State-level sector-specific agencies that provide essential services such as energy, telecommunications, water, and transportation. These State and regional partnerships develop integrated preparedness, security, and resilience plans based on a concrete risk analysis that accounts for local and regional factors.

Local critical infrastructure partnerships often link to local Chambers of Commerce, business Roundtables, or similar coalitions of private sector companies. They also include public-private partnerships, as well as community service organizations, that support preparedness, response, and recovery.

Federal, private sector, and international partners work together to implement coordinated global infrastructure security measures to protect against current and future physical and cyber threats.

[20] Domestic Security Alliance Council. http://www.dsac.gov?Pages/index.aspx

These include: sharing information; implementing existing agreements affecting critical infrastructure security and resilience; developing policies for cross-border coordination of security and resilience initiatives; addressing cross-sector and global issues such as cybersecurity; and enhancing understanding of cross-border interdependencies of critical infrastructure.

Appendix B. Roles, Responsibilities, and Capabilities of Critical Infrastructure Partners and Stakeholders

PPD-21 states, "An effective national effort to strengthen critical infrastructure security and resilience must be guided by a national plan that identifies roles and responsibilities and is informed by the expertise, experience, capabilities, and responsibilities of the SSAs, other Federal departments and agencies with critical infrastructure roles, SLTT entities, and critical infrastructure owners and operators."

This appendix includes the Federal roles and responsibilities defined in PPD-21 and described in the document *Critical Infrastructure Security and Resilience Functional Relationships,* developed by the Department of Homeland Security's Integrated Task Force and released in June 2013. Some additional roles and responsibilities described in the 2009 NIPP remain applicable and also are included here, for the Federal Government, critical infrastructure owners and operators, SLTT governments, advisory councils and committees, and academic and research organizations. These roles and activities are not intended as requirements for any partner or stakeholder group. Many of the roles and responsibilities described below represent capabilities that various partners bring to critical infrastructure security and resilience and are provided for reference to support a common awareness of the roles and contributions of various participants within the critical infrastructure community.

There are certain roles and capabilities that are shared across various partner groups. These are repeated (and tailored where appropriate) for each partner to which they apply, which introduces some redundancy to this appendix. However, this approach allows members of the critical infrastructure community to consult the section of this appendix that is most applicable to their place in the partnership and find all their potential roles and capabilities in one place.

Secretary of Homeland Security

The Secretary of Homeland Security provides strategic guidance, promotes a national unity of effort, and coordinates the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. In carrying out the responsibilities of the Homeland Security Act of 2002, as amended, the Secretary of Homeland Security:

- Evaluates national capabilities, opportunities, and challenges in securing and making resilient critical infrastructure;
- Analyzes threats to, vulnerabilities of, and potential consequences from all hazards on critical infrastructure;
- Identifies security and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors;
- Develops a national plan and metrics, in coordination with SSAs and other critical infrastructure partners;
- Integrates and coordinates Federal cross-sector security and resilience activities;
- Identifies and analyzes key interdependencies among critical infrastructure sectors; and
- Reports on the effectiveness of national efforts to strengthen the Nation's security and resilience posture for critical infrastructure.

The Secretary of Homeland Security is the principal Federal official for domestic incident management and coordinates Federal preparedness activities in alignment with PPD-8, including coordinating Federal Government responses to significant cyber or physical incidents affecting critical infrastructure (consistent with statutory authorities). The Secretary of Homeland Security coordinates with other relevant members of the Executive Branch, as appropriate, to support a single, comprehensive approach to domestic incident management so that all levels of government across the Nation have the capability to work efficiently and effectively together, using a national approach to domestic incident management.

Additional roles and responsibilities of the Secretary of Homeland Security include:

- Identify and prioritize critical infrastructure, considering physical and cyber threats, vulnerabilities, and consequences, in coordination with SSAs and other Federal departments and agencies;
- Maintain national critical infrastructure centers that shall provide a situational awareness capability that includes integrated, actionable information about emerging trends, imminent threats, and the status of incidents that may impact critical infrastructure;
- In coordination with SSAs and other Federal departments and agencies, provide analysis, expertise, and other technical assistance to critical infrastructure owners and operators and facilitate access to and exchange of information and intelligence necessary to strengthen the security and resilience of critical infrastructure;
- Conduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the SSAs and in collaboration with SLTT entities and critical infrastructure owners and operators;
- Coordinate Federal Government responses to significant cyber or physical incidents affecting critical infrastructure consistent with statutory authorities;
- Support the Attorney General and law enforcement agencies with their responsibilities to investigate and prosecute threats to and attacks against critical infrastructure;
- Coordinate with and utilize the expertise of SSAs and other appropriate Federal departments and agencies to map geospatially, image, analyze, and sort critical infrastructure by employing commercial satellite and airborne systems, as well as existing capabilities within other departments and agencies; and
- Report annually on the status of national critical infrastructure efforts as required by statute.
- Coordinating, facilitating, and supporting the overall process for building partnerships and leveraging sector-specific security expertise, relationships, and resources across critical infrastructure sectors, including oversight and support of the critical infrastructure partnership; cooperating with Federal, State, local, tribal, territorial, and regional partners; and collaborating with the Department of State to reach out to foreign governments and international organizations to strengthen the security and resilience of U.S. critical infrastructure;
- Supporting the formation and development of regional partnerships, including promoting new partnerships, enabling information sharing, and sponsoring security clearances;
- Establishing and maintaining a comprehensive, multi- tiered, dynamic information-sharing network designed to provide timely and actionable threat information, assess-

ments, and warnings to public and private sector partners. This responsibility includes protecting sensitive information voluntarily provided by the private sector and facilitating the development of sector-specific and cross-sector information-sharing and analysis systems, mechanisms, and processes;

- Facilitating the sharing of best practices and processes, and risk assessment methodologies and tools across sectors and jurisdictions;
- Ensuring that interagency, sector, and cross-sector coordination and information-sharing mechanisms and resources are in place to support critical infrastructure-related incident management operations;
- Sponsoring critical infrastructure security and resilience-related R&D, demonstration projects, and pilot programs;
- Supporting the development and transfer of advanced technologies while leveraging private sector expertise and competencies, including participation in the development of voluntary standards or best practices, as appropriate;
- Promoting national-level critical infrastructure security and resilience education, training, and awareness in cooperation with Federal, State, local, tribal, territorial, regional, and private sector partners, and academia;
- Identifying and implementing plans and processes, in collaboration with SSAs, SCCs, and SLTT entities, for appropriate increases in security and resilience measures that align to hazard warnings and/or specific threats;
- Providing real-time (24/7) threat and incident reporting to the critical infrastructure community;
- Conducting modeling and simulations with the SSAs to analyze sector, cross-sector, and regional dependencies and interdependencies, including cyber, and sharing the results with critical infrastructure partners, as appropriate;
- Helping inform the annual Federal budget process based on critical infrastructure risk and the potential for reducing risk and need, in coordination with SSAs, GCCs, and other partners, as appropriate;
- Supporting performance measurement for the national critical infrastructure security and resilience program to encourage continuous improvement and providing annual critical infrastructure security and resilience reports to the Executive Office of the President (EOP) and Congress;
- Integrating national efforts for the security, resilience, and restoration of critical information systems and the cyber components of physical critical infrastructure, including analysis, warning, information-sharing, and risk management activities and programs;
- Working with critical infrastructure partners to define what information is useful to establish and maintain national situational awareness, including describing information-sharing objectives, analysis, prevention, detection, mitigation, response, and recovery from cyber incidents affecting critical infrastructure.
- Evaluating preparedness for critical infrastructure security and resilience across sectors and jurisdictions;
- Documenting lessons learned from exercises, actual incidents, and pre-disaster mitigation efforts and applying those lessons, where applicable, to critical infrastructure security and resilience efforts;
- Promoting critical infrastructure awareness to provide incentives for participation by

critical infrastructure owners and operators;

- Working with the Department of State, SSAs, and other partners to ensure that U.S. critical infrastructure security and resilience efforts are coordinated with international partners;
- Evaluating the need for and coordinating the security and resilience of additional critical infrastructure categories over time, as appropriate; and
- Serving as the SSA or co-SSA for 10 of the critical infrastructure sectors identified in PPD-21. Specific SSA responsibilities, as appropriate, are outlined below.

Sector-Specific Agencies

Each critical infrastructure sector has unique characteristics, operating models, and risk profiles. The Federal SSA or co-SSA assigned to each sector has institutional knowledge and specialized expertise about their sector(s). Recognizing existing statutory or regulatory authorities of specific Federal departments and agencies, and leveraging existing sector familiarity and relationships, SSAs:

- Coordinate with DHS and other relevant Federal departments and agencies and collaborate with critical infrastructure owners and operators, where appropriate with independent regulatory agencies, and with SLTT entities, as appropriate;
- Serve as a day-to-day Federal interface for the dynamic prioritization and coordination of security and resilience sector-specific activities;
- Carry out critical infrastructure incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations;
- Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate; and
- Support the Secretary of Homeland Security's statutorily required reporting requirements by providing, on an annual basis, sector-specific critical infrastructure information.

Sector-Specific Agency	Critical Infrastructure Sector
Department of Agriculture[a] Department of Health and Human Services[b]	Food and Agriculture
Department of Defense[c]	Defense Industrial Base
Department of Energy	Energy[d]
Department of Health and Human Services	Healthcare and Public Health
Department of the Treasury	Financial Services
Environmental Protection Agency	Water and Wastewater Systems
Department of Homeland Security	Chemical Commercial Facilities Communications Critical Manufacturing Dams Emergency Services Information Technology Nuclear Reactors, Materials, and Waste
Department of Homeland Security, General Services Administration	Government Facilities[e]
Department of Homeland Security, Department of Transportation	Transportation Systems

[a] The Department of Agriculture is responsible for agriculture and food (meat, poultry, and egg products).

[b] The Department of Health and Human Services is responsible for food other than meat, poultry, and egg products.

[c] Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense (DoD), including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.

[d] The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power. The Department of Homeland Security is the SSA for commercial nuclear power facilities and for dams.

[e] The Department of Education is the SSA for the Education Facilities Subsector of the Government Facilities Sector; the Department of the Interior is the SSA for the National Monuments and Icons Subsector of the Government Facilities Sector.

Additional SSA roles and capabilities include:

- Facilitating the overall process for building partnerships and leveraging critical infrastructure security expertise, relationships, and resources within the sector, as appropriate, including sector-level coordination and support of the critical infrastructure partnership described in this Plan;
- Coordinating, facilitating, and supporting comprehensive risk assessment/management programs, as appropriate, for high-risk critical infrastructure, identifying security and resilience priorities, and incorporating critical infrastructure security and resilience activities as a key component of the all-hazards approach to national preparedness

within the sector;

- Developing or revising SSPs, in collaboration with public and private sector partners, and providing sector-specific information to DHS to enable national cross-sector critical infrastructure program assessments.
- Collaborating with private sector partners and encouraging the development of appropriate voluntary information-sharing and analysis mechanisms within the sector (this includes encouraging information sharing, where possible, among private entities, as well as among public and private entities);
- Facilitating the sharing of real-time incident notification, as well as critical infrastructure security and resilience best practices and processes, and risk assessment methodologies and tools within the sector;
- Promoting critical infrastructure security and resilience education, training, and awareness within the sector in coordination with Federal, State, regional, local, tribal, territorial, and private sector partners, and academia;
- Helping inform the annual Federal budget process considering critical infrastructure risk and security needs in coordination with partners and allocating resources accordingly;
- Tracking and reporting on progress in critical infrastructure security and resilience activities within the sector to enable continuous improvement;
- Contributing to the National Critical Infrastructure Security and Resilience Research and Development Plan;
- Identifying and recommending appropriate strategies to encourage private sector participation in sector activities;
- Providing information to DHS, as appropriate, to enable national-level risk assessment and inform national-level resource allocation;
- Supporting protocols for the Protected Critical Infrastructure Information (PCII) program, as appropriate;
- Working with DHS, as appropriate, to develop and evaluate sector-specific risk assessment tools;
- Supporting dependency, interdependency, consequence, and other sector analyses, as needed;
- Coordinating with DHS and other partners to promote critical infrastructure awareness to encourage participation by critical infrastructure owners and operators;
- Promoting sector-level participation in the National Exercise Program (NEP), Homeland Security Exercise and Evaluation Program (HSEEP), and exercises sponsored by other entities;
- Assisting SLTT and other partners in their efforts to:
  - Organize and conduct security and continuity-of-operations planning, and elevate awareness and understanding of threats and vulnerabilities to their assets, systems, and networks; and
  - Identify and promote effective sector-specific best practices and methodologies;
- Supporting the identification and implementation of plans and processes within the sector for enhancements in security measures that align to all-hazard warnings and/or specific threats;
- Understanding and mitigating sector-specific risk by developing or encouraging appropriate security and resilience measures, information-sharing mechanisms, and

emergency recovery plans for physical and cyber assets, systems, and networks within the sector and interdependent sectors; and

- Coordinating with DHS, the Department of State, and other appropriate departments and agencies, to support integration of U.S. critical infrastructure security and resilience priorities and programs into regional and international venues, and address relevant dependency, interdependency, cross-border and global issues.

Other Federal Departments and Agencies

As stated in PPD-21, Federal departments and agencies shall provide timely information to the Secretary of Homeland Security and the national critical infrastructure centers necessary to support cross-sector analysis and inform the situational awareness capability for critical infrastructure; the centers will in turn share the information back with the appropriate critical infrastructure partners.

Federal departments and agencies that are not designated as SSAs, but have unique responsibilities, functions, or expertise in a particular critical infrastructure sector (such as GCC members) assist in identifying and assessing high-consequence critical infrastructure and collaborate with relevant partners to share security and resilience-related information within the sector, as appropriate.

The following departments and agencies have specialized or support functions related to critical infrastructure security and resilience that shall be carried out by, or along with, other Federal departments and agencies and independent regulatory agencies, as appropriate.

Department of State

The Secretary of State has direct responsibility for policies and activities related to the protection of U.S. citizens and U.S. facilities abroad, and has the overarching lead for U.S. foreign relations, policies, and activities as well as for the advancement of U.S. interests abroad. As part of the day-to-day diplomatic activities on behalf of the U.S. Government, the Department of State (DOS) is responsible for establishing and maintaining international partnerships that are essential to critical infrastructure security and resilience. DOS, in coordination with DHS, SSAs, and other Federal departments and agencies, coordinates with foreign governments, international organizations, and the U.S. private sector to strengthen the security and resilience of critical infrastructure located outside the United States and to facilitate the overall exchange of best practices and lessons learned for promoting the security and resilience of critical infrastructure on which the Nation depends.

Department of Defense

In support of critical infrastructure security and resilience, the Department of Defense (DoD) operates, defends, and ensures the resilience of DoD-owned or contracted critical infrastructure; defends the nation from attack in all domains, including cyber; gathers foreign intelligence and determines attribution in support of national and DoD requirements; secures national security and military systems; and investigates criminal cyber activity under military jurisdiction. The National Security Administration, as part of DoD and the Intelligence Community, provides

foreign intelligence support and information assurance support to DHS and other departments and agencies per Executive Order 12333.

Department of Justice

The Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI), leads counterterrorism and counterintelligence investigations and related law enforcement activities across the critical infrastructure sectors. DOJ investigates, disrupts, prosecutes, and otherwise reduces foreign intelligence, terrorist, and other threats to, and actual or attempted attacks on, or sabotage of, the Nation's critical infrastructure. The FBI also conducts domestic collection, analysis, and dissemination of cyber threat information, and is responsible for the operation of the National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF serves as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from DHS, the Intelligence Community, DoD, and in collaboration with the SSAs and other agencies as appropriate. The Attorney General and the Secretary of Homeland Security collaborate to carry out their respective critical infrastructure missions.

Department of the Interior

The Department of the Interior, in collaboration with the SSA for the Government Facilities Sector, identifies, prioritizes, and coordinates the security and resilience efforts for national monuments and icons and incorporate measures to reduce risk to these critical assets, while also promoting their use and enjoyment.

Department of Commerce

The Department of Commerce, in collaboration with DHS, the SSAs, and other relevant Federal departments and agencies, engages private sector, research, academic, and government organizations to improve security for technology and tools related to cyber-based systems, and promote the development of other efforts related to critical infrastructure to enable the timely availability of industrial products, materials, and services to meet homeland security requirements.

Intelligence Community

The Intelligence Community, led by the Director of National Intelligence, uses applicable authorities and coordination mechanisms to provide, as appropriate, intelligence assessments regarding threats to critical infrastructure and coordinate on intelligence and other sensitive or proprietary information related to critical infrastructure. In addition, information security policies, directives, standards, and guidelines for safeguarding national security systems are overseen as directed by the President, applicable law, and in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

General Services Administration

The General Services Administration, in consultation with DoD, DHS, and other Federal departments and agencies as appropriate, provides or supports government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure.

Nuclear Regulatory Commission

The Nuclear Regulatory Commission (NRC) oversees its licensees' protection of commercial nuclear power reactors and non-power nuclear reactors used for research, testing, and training; nuclear materials in medical, industrial, and academic settings, and facilities that fabricate nuclear fuel; and the transportation, storage, and disposal of nuclear materials and waste. The NRC collaborates, to the extent possible, with DHS, DOJ, the Department of Energy, the Environmental Protection Agency, the Department of Health and Human Services, and other Federal departments and agencies, as appropriate, on strengthening critical infrastructure security and resilience.

Federal Communications Commission

The Federal Communications Commission, to the extent permitted by law, exercise its authority and expertise to partner with DHS and the Department of State, as well as other Federal departments and agencies and SSAs as appropriate, on: (1) identifying and prioritizing communications infrastructure; (2) identifying communications sector vulnerabilities and working with industry and other stakeholders to address those vulnerabilities; and (3) working with stakeholders, including industry, and engaging foreign governments and international organizations to increase the security and resilience of critical infrastructure within the communications sector and facilitating the development and implementation of best practices promoting the security and resilience of critical communications infrastructure on which the Nation depends.

Federal and State Regulatory Agencies

Some sectors are regulated by Federal or State regulatory agencies that are not the designated SSA for the sector. In these cases, regulators play an important information-sharing role with regulated entities and possess unique insight into the functioning of the critical infrastructure they oversee. These regulatory agencies bring key capabilities to the critical infrastructure partnership, including:

- Facilitating the exchange of information with critical infrastructure owners and operators during incident response and recovery;
- Encouraging critical infrastructure owners and operators to participate in public-private partnerships (e.g., through regional coalitions);
- Participating in GCCs and coordinating with SSAs on critical infrastructure security and resilience initiatives; and
- Ensuring sector resilience through the policymaking and oversight process.

Critical Infrastructure Owners and Operators

Critical infrastructure owners and operators in the public and private sectors develop and implement security and resilience programs for the critical infrastructure under their control. Owners and operators take action to support risk management planning and investments in security as a necessary component of prudent business planning and operations. In today's risk environment, these activities generally include reassessing and adjusting business continuity and emergency management plans, building increased resilience and redundancy into business processes and systems, protecting facilities against physical and cyber attacks, reducing the vulnerability to natural disasters, guarding against insider threats, and increasing coordination with external organizations to avoid or minimize the impact on surrounding communities or other industry partners.

Addressing critical infrastructure cybersecurity is a crucial part of an all-hazards approach to risk. As such, critical infrastructure owners and operators participate in many risk mitigation activities including cybersecurity information-sharing efforts (e.g., sector-specific cyber working groups, the Cross-Sector Cybersecurity Working Group, and the Industrial Control Systems Joint Working Group), cyber risk assessments, cybersecurity exercises, cyber incident response and recovery efforts, and cyber metrics development.

For many private sector enterprises, the level of investment in security reflects risk-versus-consequence tradeoffs that are based on two factors: (1) what is known about the risk environment, and (2) what is economically justifiable and sustainable in a competitive marketplace or within resource constraints. In the context of the first factor, the Federal Government is uniquely positioned to help inform critical infrastructure investment decisions and operational planning across the sectors. Owners and operators may look to the government and information sharing and analysis organizations like ISACs as a source of security-related best practices and for attack or natural hazard indications, warnings, and threat assessments.

In relation to the second factor, owners and operators may rely on government entities or participate in collective efforts with other owners and operators to address risks outside of their property or in situations in which the current threat exceeds an enterprise's capability to protect itself or requires an unreasonable level of additional investment to mitigate risk. In this situation, public and private sector partners at all levels collaborate to address the security and resilience of national-level critical infrastructure, provide timely warnings, and promote an environment in which critical infrastructure owners and operators can carry out their specific responsibilities.

The roles of specific owners and operators vary widely within and across sectors. Some sectors have statutory and regulatory frameworks that affect private sector security operations within the sector; however, most are guided by voluntary security and resilience regimes or adherence to industry-promoted best practices.

Within this diverse security and resilience landscape, critical infrastructure owners and operators can contribute to national critical infrastructure security and resilience efforts by:

- Performing comprehensive risk assessments tailored to their specific sector, enterprise, or

facility risk landscape;

- Implementing security and resilience actions and programs to identify and mitigate vulnerabilities;
- Participating in the critical infrastructure partnership;
- Understanding critical dependencies and interdependencies at the sector, enterprise, and facility levels;
- Developing and coordinating critical infrastructure security and resilience and emergency response actions, plans, and programs with appropriate Federal, State, and local government authorities;
- Establishing continuity plans and programs that facilitate the performance of critical functions during an emergency or until normal operations can be resumed;
- Establishing cybersecurity programs and associated awareness training within the organization;
- Adhering to recognized industry best business practices and standards, including those with a cybersecurity nexus;
- Participating in Federal, State, local, and tribal government emergency management programs and coordinating structures;
- Establishing resilient, robust, and/or redundant operational systems or capabilities associated with critical functions;
- Promoting critical infrastructure security and resilience education, training, and awareness programs;
- Adopting and implementing effective workforce security assurance programs to mitigate potential insider threats;
- Contributing technical expertise to the critical infrastructure security and resilience efforts of the SSAs and DHS;
- Participating in regular critical infrastructure security and resilience-focused training and exercise programs with other public and private sector partners;
- Identifying and communicating requirements to DHS and/or the SSAs and State and local governments for critical infrastructure security and resilience-related R&D;
- Identifying and sharing security and resilience-related best practices with critical infrastructure partners;
- Sharing information to enhance situational awareness in steady state and during incidents;
- Encouraging participation in sector or cross-sector coordinating councils; and
- Working to identify and reduce barriers to effective public-private partnerships.

State, Local, Tribal, and Territorial Governments and Regional Organizations

State, local, tribal, and territorial governments are responsible for implementing the homeland security mission, protecting public safety and welfare, and ensuring the provision of essential services to communities and industries within their jurisdictions. They also play a very important role in ensuring the security and resilience of critical infrastructure under their control, as well as that owned and operated by other parties within their jurisdictions. The efforts of these public entities are critical to the effective planning and implementation of critical infrastructure security and resilience activities. Since State, local, tribal, and territorial officials are often the first on the scene of an incident, they are critical to time-sensitive, post-

event critical infrastructure response and recovery activities.

Critical infrastructure security and resilience programs form an essential component of State, local, tribal, and territorial homeland security strategies, particularly with regard to establishing funding priorities and informing security and resilience investment decisions. To facilitate effective critical infrastructure security and resilience and performance measurement, these programs should reference all core elements of this Plan, where appropriate, including key cross-jurisdictional security and information-sharing linkages, as well as specific critical infrastructure security and resilience programs focused on risk management. These programs play a primary role in the identification and protection of critical infrastructure regionally and locally and also support DHS and SSA efforts to identify, ensure connectivity with, and enable the security and resilience of critical infrastructure of national significance within the jurisdiction.

State and Territorial Governments

State and territorial governments are responsible for establishing partnerships, facilitating coordinated information sharing, and enabling planning and preparedness for critical infrastructure security and resilience within their jurisdictions. They serve as crucial coordination hubs, bringing together prevention, protection, response, and recovery authorities, capabilities, and resources among local jurisdictions, across sectors, and between regional entities. States and territories also act as conduits for requests for Federal assistance when the threat or incident situation exceeds the capabilities of public and private sector partners at lower jurisdictional levels. States receive critical infrastructure information from the Federal Government to support national and State critical infrastructure security and resilience programs.

State and territorial programs should address all relevant aspects of critical infrastructure security and resilience, leverage support from homeland security assistance programs that apply across the homeland security mission area, and reflect priority activities in their strategies to ensure that resources are effectively allocated. Effective statewide and regional critical infrastructure security and resilience efforts should be integrated into the overarching homeland security program framework at the State or territory level to ensure that prevention, protection, response, and recovery efforts are synchronized and mutually supportive.

Critical infrastructure security and resilience at the State or territorial level must cut across all sectors present within the State or Territory and support national, State, and local priorities. The program also should explicitly address unique geographical issues, including trans-border concerns, as well as interdependencies among sectors and jurisdictions within those geographical boundaries.

Specific State and territorial activities for critical infrastructure security and resilience may include, but are not limited to:

- Acting as a focal point for and promoting the coordination of security, resilience, and emergency response activities, preparedness programs, and resource support among local jurisdictions, regional organizations, and private sector partners;

- Developing a consistent approach to critical infrastructure identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant stakeholders within their jurisdictions;
- Identifying, implementing, and monitoring a risk management approach and taking corrective actions, as appropriate;
- Participating in significant national, regional, and local awareness programs to encourage appropriate management and security of cyber systems;
- Working with State-level sector-specific agencies to support the vision, mission, and scope of this plan, as appropriate, within their sectors, and to engage subject matter experts at the sector level in State government to assist with this effort;
- Acting as conduits for requests for Federal assistance when the threat or current situation exceeds the capabilities of State and local jurisdictions and the private entities resident within them;
- Facilitating the exchange of security information, including threat assessments and other analyses, attack indications and warnings, and advisories, within and across jurisdictions and sectors therein;
- Participating in the critical infrastructure partnership, including: sector-specific GCCs; the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC); SCCs; and other critical infrastructure governance and planning efforts relevant to the given jurisdiction;
- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve the critical infrastructure security and resilience mission in accordance with relevant plans and strategies;
- Sharing information on infrastructure deemed to be critical from national, State, regional, local, tribal, and/or territorial perspectives to enable prioritized security and restoration of critical public services, facilities, utilities, and functions within the jurisdiction;
- Addressing unique geographical issues, including trans-border concerns, dependencies, and interdependencies among the sectors within the jurisdiction;
- Identifying and implementing plans and processes for increasing security measures that align to all-hazard warnings and/or specific threats;
- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual incidents, and applying that learning, where applicable, to the critical infrastructure context;
- Coordinating with partners to promote education, training, and awareness of critical infrastructure security and resilience to motivate increased participation by owners and operators;
- Providing response and security support, as appropriate, where there are gaps and where local entities lack the resources needed to address those gaps;
- Identifying and communicating the requirements for critical infrastructure-related R&D to DHS; and
- Providing information, as part of the grants process and/or homeland security strategy updates, regarding State priorities, requirements, and critical infrastructure-related funding needs.

Local Governments

Local governments represent the front lines for homeland security and, more specifically, critical infrastructure security and resilience. They provide critical public services and functions in conjunction with private sector owners and operators. In some sectors, local government entities, through their public works departments, own and operate critical infrastructure such as water, storm water, and electric utilities. Most disruptions or malevolent acts that affect critical infrastructure begin and end as local situations. Local authorities typically shoulder the weight of initial prevention, response, and recovery operations until coordinated support from other sources becomes available, regardless of who owns or operates the affected asset, system, or network. As a result, local governments are key players within the critical infrastructure partnership. They drive emergency preparedness, as well as local participation in critical infrastructure security and resilience across a variety of jurisdictional partners, including government agencies, owners and operators, and private citizens in the communities that they serve.

Local government activities for critical infrastructure security and resilience may include, but are not limited to:

- Acting as a focal point for and promoting the coordination of security, resilience, and emergency response activities, preparedness programs, and resource support among local agencies, businesses, and citizens;
- Developing a consistent approach at the local level to critical infrastructure identification, risk determination, mitigation planning, and prioritized security investment, and exercising preparedness among all relevant partners within the jurisdiction;
- Identifying, implementing, and monitoring a risk management plan, and taking corrective actions, as appropriate;
- Participating in significant national, State, local, and regional education and awareness programs to encourage appropriate management and security of cyber systems;
- Facilitating the exchange of security information, including threat assessments, attack indications, warnings, and advisories, among partners within the jurisdiction;
- Participating in the critical infrastructure partnership, including GCCs, SCCs, SLTTGCC, and other critical infrastructure structures relevant to the given jurisdiction;
- Ensuring that funding priorities are addressed and that resources are allocated efficiently and effectively to achieve the critical infrastructure security and resilience mission in accordance with relevant plans and strategies;
- Establishing continuity plans and programs that facilitate the performance of critical functions during an emergency or until normal operations can be resumed;
- Sharing information with partners, as appropriate, on infrastructure deemed to be critical from the local perspective to enable prioritized security and restoration of critical public services, facilities, utilities, and processes within the jurisdiction;
- Addressing unique geographical issues, including trans-border concerns, dependencies, and interdependencies among agencies and enterprises within the jurisdiction;
- Identifying and implementing plans and processes for increases in security measures that align to all-hazard warnings and/or specific threats;
- Documenting lessons learned from pre-disaster mitigation efforts, exercises, and actual

incidents, and applying that learning, where applicable, to the critical infrastructure security and resilience context;
- Conducting critical infrastructure security and resilience public awareness activities; and
- Working with State/territorial cabinet agencies to ensure that all pertinent sector partners are represented.

Tribal Governments

Tribal government roles and capabilities regarding critical infrastructure security and resilience generally mirror those of State and local governments as detailed above. Tribal governments are responsible for the public health, welfare, and safety of tribal members, as well as the security of critical infrastructure and the continuity of essential services under their jurisdiction. Within the critical infrastructure partnership, tribal governments coordinate with Federal, State, local, and international counterparts to achieve synergy in the implementation of critical infrastructure security and resilience frameworks within their jurisdictions. This is particularly important in the context of information sharing, risk analysis and management, awareness, preparedness planning, and security and resilience program investments and initiatives.

Regional Organizations

Regional partnerships include a variety of public-private sector initiatives that cross jurisdictional and/or sector boundaries and focus on prevention, protection, mitigation, response, and recovery within or serving the population of a defined geographical area. Specific regional initiatives range in scope from organizations that include multiple jurisdictions and industry partners within a single State to groups that involve jurisdictions and enterprises in more than one State and across international borders. In many cases, State governments also collaborate through the adoption of interstate compacts to formalize regionally based partnerships regarding critical infrastructure security and resilience.

Partners leading or participating in regional initiatives are encouraged to capitalize on the larger area- and sector-specific expertise and relationships to:

- Promote collaboration among partners in implementing critical infrastructure risk assessment and management activities;
- Facilitate education and awareness of critical infrastructure security and resilience efforts occurring within their geographical areas;
- Participate in regional exercise and training programs, including a focus on critical infrastructure security and resilience collaboration across jurisdictional and sector boundaries;
- Support threat-initiated and ongoing operations-based activities to enhance security and resilience, as well as to support mitigation, response, and recovery;
- Work with State, local, tribal, territorial, and international governments and the private sector, as appropriate, to evaluate regional and cross-sector critical infrastructure interdependencies, including cyber considerations;
- Conduct the appropriate regional planning efforts and undertake appropriate partnership agreements to enable regional critical infrastructure security and resilience activities and

enhanced response to emergencies;

- Facilitate information sharing and data collection between and among regional initiative members and external partners;
- Share information on progress and critical infrastructure security and resilience requirements with DHS, the SSAs, State and local governments, and other critical infrastructure partners, as appropriate; and
- Participate in the critical infrastructure partnership.

State and Regionally Based Boards, Commissions, Authorities, Councils, and Other Entities

An array of boards, commissions, authorities, councils, and other entities at the State, local, tribal, and regional levels perform regulatory, advisory, policy, or business oversight functions related to various aspects of critical infrastructure operations and security within and across sectors and jurisdictions. Some of these entities are established through State- or local-level executive or legislative mandates with elected, appointed, or voluntary membership. These groups include, but are not limited to, transportation authorities, public utility commissions, water and sewer boards, park commissions, housing authorities, public health agencies, and many others. These entities may serve as State-level sector-specific agencies and contribute expertise, assist with regulatory authorities, or help facilitate investment decisions related to critical infrastructure security and resilience efforts within a given jurisdiction or geographical region.

Advisory Councils

Advisory councils provide advice, recommendations, and expertise to the government (e.g., DHS, SSAs, and State or local agencies) regarding critical infrastructure security and resilience policy and activities. These entities also help enhance public-private partnerships and information sharing. They often provide an additional mechanism to engage with a pre-existing group of private sector leaders to obtain feedback on critical infrastructure security and resilience policy and programs, and to make suggestions to increase the efficiency and effectiveness of specific government programs. Examples of critical infrastructure security and resilience-related advisory councils and their associated roles include:

- **Homeland Security Advisory Council (HSAC)**: HSAC provides advice and recommendations to the Secretary of Homeland Security on relevant issues. The Council members, appointed by the DHS Secretary, include experts from State and local governments, public safety, security and first-responder communities, academia, and the private sector.
- **Private Sector Senior Advisory Committee (PVTSAC)**: The Secretary of Homeland Security established PVTSAC as a subcommittee of HSAC to provide HSAC with expert advice from leaders in the private sector.
- **National Infrastructure Advisory Council (NIAC)**: NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of physical and cyber systems across all critical infrastructure sectors. The council comprises up to 30 members appointed by the President. Members are selected from the private sector, academia, and State and local governments. The council was established (and amended) under Executive Orders 13231, 13286, and 13385.
- **National Security Telecommunications Advisory Committee (NSTAC)**: NSTAC

provides industry-based advice and expertise to the President on issues and problems related to implementing National Security and Emergency Preparedness (NS/EP) communications policy. NSTAC, created under Executive Order 12382, comprises up to 30 industry chief executives representing the major communications and network service providers and information technology, finance, and aerospace companies.

Academia and Research Centers

The academic and research communities play an important role in enabling national-level critical infrastructure security and resilience, including:

- Establishing Centers of Excellence (i.e., university-based partnerships or federally funded R&D centers) to provide independent analysis of critical infrastructure security and resilience issues;
- Supporting the research, development, testing, evaluation, and deployment of security and resilience technologies;
- Supporting development and implementation of concepts, architectures, and technical strategies associated with critical infrastructure security and resilience;
- Analyzing, developing, and sharing best practices related to critical infrastructure prioritization, security, and resilience efforts;
- Researching and providing innovative thinking and perspective on threats and the behavioral aspects of terrorism and criminal activity;
- Preparing or disseminating guidelines and descriptions of best practices for physical and cyber security;
- Developing and providing suitable all-hazards risk analysis and risk management courses for critical infrastructure security and resilience professionals;
- Establishing undergraduate and graduate curricula and degree programs;
- Conducting research to identify new technologies and analytical methods that can be applied by partners to support critical infrastructure security and resilience efforts;
- Participating in the review and validation of critical infrastructure security and resilience risk analysis and management approaches; and
- Engaging and serving as a resource to local communities for efforts to enhance the security and resilience of physical and cyber critical infrastructure.