National Critical Infrastructure Security and Resilience Research and Development Plan

Homeland Security

November 2015

Table of Contents

Executive Summary

In February 2013, President Obama issued Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (PPD-21) and Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*. The coordinated release of these two policies underscores the Administration's commitment to integrating cyber and physical security and strengthening resilience across interrelated systems.

PPD-21 directed the Secretary of the Department of Homeland Security (DHS), in coordination with the Office of Science and Technology Policy, Sector-Specific Agencies, the Department of Commerce, and other Federal departments and agencies, to provide to the President a National Critical Infrastructure Security and Resilience Research and Development Plan (hereafter the National CISR R&D Plan or the Plan) that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments.

The National CISR R&D Plan shares the strategic vision for CISR established in the National Infrastructure Protection Plan (NIPP) 2013[1] of "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 hastened."

Recognizing that future R&D activities are a key component of implementing the policy set forth in PPD-21 and achieving the NIPP goals, this Plan has the following primary objectives:

- *Take into account the diverse structure of critical infrastructure, the evolving threat landscape, and annual metrics to identify priorities and guide R&D requirements and investments.*
- *Build upon the existing guidance in PPD-21, NIPP 2013, and other relevant policy documents, to focus national R&D efforts toward strengthening critical infrastructure security and resilience.*

The National CISR R&D Plan identifies ten guiding tenets that enable CISR R&D efforts across the critical infrastructure community, recognizing that critical infrastructure stakeholders must protect privacy and civil liberties when planning and executing R&D activities.

The Plan builds on past and ongoing CISR R&D activities across the critical infrastructure community, including extensive efforts by government, the private sector, and academia. The National CISR R&D Plan is intended to reinforce and augment successful advances in CISR R&D and identify and fill gaps and unmet needs through active collaboration with stakeholders.

The ability to identify and assess threats and hazards, address them before and as they arise, and understand and quantify the related consequences is a critical element of risk management and a primary driver for CISR R&D efforts. The National CISR R&D Plan provides an overview of the risk environment and emphasizes the need to sustain and grow partnerships to enable a collaborative approach to managing critical infrastructure risk.

[1] *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, U.S. Department of Homeland Security, December 2013.

The National CISR R&D Plan draws on various sources, including relevant national plans and strategies, public feedback through Federal Register Notices and online forums, and related recommendations from Presidential advisory groups. The Plan represents input and ideas from a range of partners and stakeholders who were involved through working groups and outreach sessions throughout the development process. DHS facilitated a workshop in November 2014 that brought together stakeholders from across the critical infrastructure sectors to discuss key focus areas for the Plan. These discussions generated the idea of using grand-scale R&D challenges as a way to identify the R&D priorities called for in PPD-21.

Building on the workshop discussions and feedback received through stakeholder outreach and engagement, five overarching R&D topics emerged that represent the National CISR R&D Priority Areas, as follows:

- **Develop the foundational understanding of critical infrastructure systems and systems dynamics;**
- **Develop integrated and scalable risk assessment and management approaches;**
- **Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure;**
- **Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action;**
- **Build a crosscutting culture of CISR R&D collaboration.**

These Priority Areas are intended to inform R&D investments, promote innovation, and guide research across the critical infrastructure community. They support the development of both evolutionary and transformative R&D solutions to enhance the security and resilience of critical infrastructure.

The National CISR R&D Plan also identifies enabling activities necessary to guide and execute CISR R&D, including collaboration, information sharing, and the measurement of progress. Recognizing that no single sector or entity can advance the National CISR R&D Priority Areas on its own, public and private stakeholders should work collaboratively to define R&D requirements and design and implement solutions that meet identified needs. Sharing information on threats and hazards, effective risk management strategies, and operational best practices can help reduce risk and guide R&D investments. The critical infrastructure community should develop reliable measures for evaluating the effectiveness of R&D activities in advancing the National CISR R&D Priority Areas.

The National CISR R&D Plan is intended to strengthen national CISR R&D efforts and outcomes, through collaboration, partnership, and information sharing. Through a coordinated national approach, the critical infrastructure community can establish R&D priorities, leverage investments, and accelerate transition to practice, now and into the future.

1. Introduction

Background

On February 12, 2013, President Obama signed Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (PPD-21), describing a national effort to secure and strengthen the resilience of the Nation's critical infrastructure. The President also issued Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity* in February 2013, which calls on the Federal Government to work closely with critical infrastructure owners and operators to improve information sharing and collaboratively develop and implement risk-based approaches to cybersecurity. The coordinated release of these two policies underscores the Administration's commitment to integrating cyber and physical security and augmenting protective measures with additional emphasis on strengthening resilience across interrelated systems.

PPD-21 directs the Secretary of the Department of Homeland Security (DHS), in coordination with the White House Office of Science and Technology Policy, Sector-Specific Agencies (SSAs), the Department of Commerce, and other Federal departments and agencies, to "provide to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a National Critical Infrastructure Security and Resilience Research and Development Plan that takes into account the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments. The plan should be issued every 4 years after its initial delivery, with interim updates as needed."

Overview

The purpose of this *National Critical Infrastructure Security and Resilience Research and Development Plan* (hereafter referred to as the National CISR R&D Plan or the Plan) is to identify National R&D Priority Areas that inform R&D investments, promote innovation, and guide research activities across the critical infrastructure community. The critical infrastructure community includes public and private critical infrastructure owners and operators; Federal departments and agencies, including SSAs; State, local, tribal, and territorial (SLTT) governments and regional entities; and other organizations from the private and non-profit sectors, including research and educational institutions and, in some cases, international partners and organizations. Future CISR R&D activities should be driven by continued collaborative efforts aimed at strengthening the security and resilience of critical infrastructure.

Considering the essential connections that exist between the goods and services provided by critical infrastructure and the competitiveness and vitality of the national economy, this Plan highlights the need to consider the dynamic linkages among the interdependent infrastructure systems that underpin American society. This Plan recognizes the Nation's reliance on critical infrastructure, especially in urban areas, and promotes action to develop and deploy technologies and solutions to manage critical infrastructure risk at the local, regional, and national levels. By employing more localized, "place-based" strategies in addition to broader-scale programs at the regional and national levels, the critical infrastructure community can leverage redundancies in managing risk and improve the Nation's adaptability and resilience.

This Plan employs an intentionally expansive perspective when considering the range of potential CISR R&D topics. R&D for CISR can encompass a broad range of activities, including but not limited to: characterizing infrastructure systems to build an integrated systems understanding; developing technology solutions to secure and enhance the resilience of cyber and physical systems; researching and establishing

policies and regulations that enable and incentivize CISR enhancements; and applying social and behavioral sciences to model and manage the human role in CISR. This Plan also identifies enabling activities necessary for advancing the CISR R&D Priority Areas. Critical infrastructure stakeholders should leverage existing partnership structures and develop new working relationships as needed to help guide and execute R&D efforts. Active collaboration supports information sharing, which is also a core enabler for R&D activities.

The audience for this National CISR R&D Plan includes the broad critical infrastructure community and others with an interest in advancing future R&D for the security and resilience of the Nation's critical infrastructure. This Plan supports a national effort to develop capabilities that reduce critical infrastructure risk and enhance resilience to threats and hazards. By pursuing a coordinated and collaborative approach, the critical infrastructure community can establish R&D requirements and priorities, leverage investments, accelerate transition to practice, and innovate to meet future needs.

The 16 critical infrastructure sectors identified in PPD-21 provide the essential products and services that support the Nation's safety, prosperity, and well-being. This Plan establishes CISR R&D Priority Areas that rise to a national level, because they are likely to improve the security and resilience of critical lifeline functions[2] or because they address threats and hazards facing one or more sectors that could cause broad regional or national-level consequences. These National CISR R&D Priority Areas are intended to serve as a broad, overarching construct under which ongoing activities can continue and future innovative endeavors can develop over time. By contrast, sector-level R&D priorities address threats, hazards, and vulnerabilities or gaps in knowledge and capabilities deemed important by sectors, subsectors, and individual critical infrastructure entities.

PPD-21 and the National Infrastructure Protection Plan (NIPP) 2013: *Partnering for Critical Infrastructure Security and Resilience* (hereafter NIPP 2013) specifically identify innovation and R&D as critical components for achieving the desired outcome of secure, functioning, and resilient critical infrastructure. CISR R&D activities also contribute to national preparedness, as established in Presidential Policy Directive 8.

This National CISR R&D Plan identifies a vision, objectives, and 10 R&D tenets to focus the scope of future research activities. The five overarching CISR R&D Priority Areas define future capabilities that are intended to drive significant advances in critical infrastructure security and resilience across all sectors. The Priority Areas and tenets taken together will guide the development of future R&D activities over the short (1-3 years), medium (3-10 years), and long term (10 years or more).

The National CISR R&D Plan is organized in the following manner:

- **Section 2 - *Vision, Objectives, and Tenets***: Outlines the vision, objectives, and R&D tenets of the National CISR R&D Plan.
- **Section 3 - *Summary of the Critical Infrastructure Risk Environment*:** Describes the evolving risk environment that drives CISR R&D.
- **Section 4 - *National CISR R&D Priority Areas*:** Describes the five National CISR R&D Priority Areas and more specific example priorities within each area, including potential supporting activities.

[2] Lifeline functions include communications, energy, transportation, and water (*NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, U.S. Department of Homeland Security, December 2013).

- **Section 5 - *Advancing the National CISR R&D Priority Areas*:** Describes the importance of partnerships and identifies example collaborative activities that can help to create an environment supportive of CISR R&D.
- **Section 6 - *Conclusion and Path Forward*:** Summarizes the way forward, including future updates to the National CISR R&D Plan and activities to support Plan implementation.

Plan Development Process

The National CISR R&D Plan was developed in collaboration with partners and stakeholders across the critical infrastructure community. DHS conducted outreach primarily through the EO-PPD Integrated Task Force R&D Working Group, composed of representatives from the private sector and Federal departments and agencies with key roles in CISR, and led by senior leadership in the DHS Science and Technology Directorate (S&T).

Among other outreach activities, a cross-sector workshop held in November 2014 brought together public and private stakeholders for an open discussion around the key focus areas for the Plan. Additional dialogue with the SSAs promoted alignment of crosscutting National CISR R&D Priority Areas with the sector-level priorities identified through sector-specific planning efforts. DHS engaged all the critical infrastructure cross-sector partnership structures in the development and review of this Plan, including the Federal Senior Leadership Council; the Critical Infrastructure Cross-Sector Council; the State, Local, Tribal, and Territorial Government Coordinating Council; and the Regional Consortium Coordinating Council.

S&T issued two Federal Register Notices[3] requesting public input on specific R&D topics and questions. A web-based crowd-sourcing campaign offered opportunities for the public and stakeholder community to suggest ideas for inclusion in the Plan. In addition, two Presidential advisory groups, including the National Infrastructure Advisory Council and the National Security Telecommunications Advisory Committee, recently provided recommendations related to CISR R&D that informed the development of this Plan. The National CISR R&D Plan also incorporates R&D recommendations and guidance from relevant national plans and strategies.

The R&D Priority Areas presented in this Plan are intended to provide a common focal point for CISR R&D efforts. It is recognized that individual sectors and stakeholders will continue to pursue a variety of security and resilience R&D activities, as appropriate to their unique risk and operating environments. The goals established for certain R&D activities serve to advance current knowledge and capabilities through evolutionary changes that refine existing technologies and paradigms. More pervasive R&D challenges can require advances that may be disruptive in nature, representing revolutionary or radical departures from current assumptions and accepted approaches. While it may be difficult or impossible to predict where and when a more disruptive or innovative solution will emerge, researchers and academics should be encouraged to expand the boundaries of current knowledge in an effort to address such challenges. This Plan should inform current and future R&D direction in support of CISR and complement public and private R&D activities and programs in these areas.

[3] Federal Register (78 FR 73202), December 5, 2013; and (79 FR 68457), November 17, 2014.

2. Vision, Objectives, and Tenets

Vision

The National CISR R&D Plan shares the strategic vision for CISR established in NIPP 2013, recognizing that future R&D activities will be a key component of implementing the policy set forth in PPD-21 and achieving the NIPP goals.

> *"A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened."*
>
> Source: NIPP 2013

Objectives

Derived from the vision, and in direct response to the requirements contained in PPD-21, the National CISR R&D Plan has two primary objectives:

- *Take into account the diverse structure of critical infrastructure, the evolving threat landscape, and annual metrics to identify priorities and guide R&D requirements and investments.*
- *Build upon the existing guidance in PPD-21, NIPP 2013, and other relevant policy documents, to focus national R&D efforts toward strengthening critical infrastructure security and resilience.*

Tenets

The National CISR R&D Plan establishes R&D tenets, representing enabling principles for CISR R&D that apply across the critical infrastructure community. Critical infrastructure stakeholders must plan and coordinate R&D activities in a manner that ensures privacy and protects civil liberties.

The CISR R&D Tenets are as follows:

- *Foundational research is required to advance understanding of critical areas in developing comprehensive and effective CISR solutions;*
- *The increasingly interconnected and interdependent nature of critical infrastructure must be better understood and addressed in an integrated and holistic manner, including the identification of systemic as well as localized risks;*
- *Integrated multidisciplinary and interdisciplinary teams can properly define the specific security and resilience challenge to be solved, specify performance and design requirements, and characterize desired outcomes;*

- *Approaches for addressing immediate near-term challenges posed by the behavior of increasingly complex cyber and physical systems and the effects of vulnerable and aging physical assets and legacy systems must complement approaches for addressing challenges of climate change adaptation and resilience;*
- *Sharing past, ongoing, and proposed R&D activities across the critical infrastructure community and broadly disseminating significant R&D advances can help inform and coordinate research activities and streamline cross-sector planning efforts;*
- *Metrics, standard methods of assessment, and baselines must continue to be developed and refined to effectively measure resilience;*
- *CISR tools, methodologies, and data must be readily available, properly secure, and useable—or easily tailored for use—by operational entities, including SLTT governments and critical infrastructure owners and operators;*
- *The development of complementary and comprehensive risk assessment methodologies across the critical infrastructure community will enable the effective and coordinated application of resources;*
- *The resources involved in creating a critical infrastructure environment that is secure and resilient to all hazards, particularly considering the scale and complexity of climate change as well as long-term risks and dynamics, necessitate rigorous, prospective risk/resilience analytical capabilities and tools to coordinate investment strategies;*
- *CISR R&D must accelerate and build innovation capacity, fostering groundbreaking, significant, and scalable research, and the development of innovative designs and technologies to achieve inherently regenerative and sustainable outcomes.*

R&D efforts for CISR must empower the critical infrastructure community to provide the technologies and tools needed by the larger community of interest and society at large to achieve the CISR R&D vision of "A Nation in which physical and cyber critical infrastructure remain secure and resilient, with vulnerabilities reduced, consequences minimized, threats identified and disrupted, and response and recovery hastened." In addition to the vision, objectives, and tenets described above, the critical infrastructure risk environment, described in Section 3, provides context for and informs the National CISR R&D Priority Areas presented in Section 4.

3. Summary of the Critical Infrastructure Risk Environment

This section provides a high-level summary of the critical infrastructure risk environment and the current state of critical infrastructure risk management as the background against which the CISR R&D Priority Areas were developed. As stated in NIPP 2013, "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 on the most effective solutions available when allocating limited resources in both steady-state and crisis operations."

The identification and assessment of threats, hazards, and vulnerabilities and the ability to understand and quantify related consequences are critical elements of risk management. The need to strengthen the ability of the critical infrastructure community to perform such activities was a driving factor in the selection of the National CISR R&D Priority Areas. In addition to known threats and hazards, risk is also introduced by ongoing changes in the operating environment, such as technological advances that may introduce new vulnerabilities, and the increased interdependency and interconnectedness of infrastructure systems across sectors, jurisdictions, and even national borders. Risks also can arise from an inability to identify and leverage opportunities to enhance resilience, including adaptive capacity.

Analysis of risk is multifaceted and based upon uncertain and constantly evolving threats and vulnerabilities. The security and resilience of the Nation's critical infrastructure continue to improve based in part on past R&D activities that increased our understanding of cyber and physical risks. The development of secure and resilient technologies and more effective and coordinated policies and programs at all levels of government also help to reduce critical infrastructure risk. At the same time, risks continue to evolve, increasing in complexity, scale, and potential consequences. In some cases, it may take decades to design and construct critical infrastructure systems. The comparatively rapid pace of change in technology, coupled with growing infrastructure interdependencies and the unpredictability of the natural and operating environment, further complicate the effective management of critical infrastructure risk.

The 2011 Strategic National Risk Assessment (SNRA) evaluated known threats and hazards that have the potential to significantly impact homeland security and grouped these into three categories: natural, technological/accidental, and adversarial/human-caused. In addition to the episodic events identified in the SNRA, the CISR R&D Priority Areas consider threats and hazards that result from lasting changes to the operating environment, including economic, environmental, and societal dynamics such as urbanization and climate change. Infrastructure vulnerability is exacerbated by interdependence and aging, both of which can magnify the consequences of a single event. A failure in an interdependent system can have cascading effects on other systems and sectors, potentially disrupting the delivery of multiple essential goods and services. One goal of building a more integrated, holistic understanding of the risk environment is to enable targeted, early interventions in the form of infrastructure investment or other activities designed to forestall escalation of disruptions and prevent larger losses.

Natural systems play an important part in defining the risk environment. Natural disasters, such as hurricanes, floods, earthquakes, and tornadoes; space weather events; and pandemics continue to pose significant risk to the Nation's critical infrastructure. The Nation is already experiencing the effects of climate change, such as sea level rise, temperature fluctuations, and changes in precipitation, which also increase risk to critical infrastructure systems.[4]

Accidents and technological failures, such as dam breaches and chemical spills, have the potential to cause loss of life and significant economic impacts. Aging and failing infrastructure can have adverse effects on security, community resilience, and public safety. CISR R&D must address the security and resilience of existing infrastructure and inform the design and construction of new infrastructure, to include consideration of interdependencies, evolving risks, and changing societal needs.

Adversarial or intentional human-caused events include insider threats and attacks using explosives or other weapons by terrorist organizations, criminal groups, or lone actors. These attacks may include the intentional release of chemical or biological agents, or the detonation of nuclear or radiological devices. Malicious actors continue to launch increasingly sophisticated attacks in cyberspace. As stated in EO 13636, "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront." As use of the Internet continues to expand, so does the critical infrastructure risk profile.

The continuous evolution of the critical infrastructure operating environment presents both risks and opportunities. For example, the interdependence of critical infrastructure increases the vulnerability to attack or breakdown, which may result in cascading failures across related systems. In addition, the rapid expansion of the use of information and communications technologies (ICT) in all sectors has dramatically increased operational efficiency, reliability, and safety through improved control and situational awareness, while simultaneously creating new vulnerabilities and threat vectors. The growing reliance of all sectors on ICT increases the number, frequency, and type of interactions between cyber and physical systems. Disruptions to interactions that are essential to continuity of operations could degrade performance and result in interruption or cessation of service.

Humans and their actions or inactions complicate the identification and management of risk for organizations. Factors affecting how and when an individual recognizes and responds to an abnormal situation—whether physical or cyber-based—may influence the actions taken and the timeliness of response. Coordination among stakeholders to execute and transition R&D into operational use enhances the ability of critical infrastructure owners and operators to manage the risks associated with these factors.

A coordinated national effort for CISR R&D includes a cross-sector culture of collaboration and partnership to support secure information sharing for improved situational awareness. As described in Section 5, various sectors and partners contribute different capabilities and perspectives to identify the most pressing R&D needs and to work jointly to advance resulting priorities. Engaging critical infrastructure owners and operators is vital to ensure that the research community understands their unique risks and operational requirements. This collaborative approach will guide the execution of R&D activities and speed the adoption of new technologies and solutions to enhance CISR.

[4] Melillo, Jerry M., Terese (T.C.) Richmond, and Gary W. Yohe, Eds., 2014: *Climate Change Impacts in the United States: The Third National Climate Assessment.* U.S. Global Change Research Program, 841 pp. doi:10.7930/J0Z31WJ2.

4. National CISR R&D Priority Areas

As referenced in Section 1, DHS S&T facilitated a National CISR R&D Plan Workshop in November 2014 that brought together stakeholders from across the critical infrastructure sectors to discuss the key areas of focus for this Plan. These discussions generated the idea of grand-scale R&D challenges as an organizing principle for the National CISR R&D Priority Areas called for in PPD-21. Building on the concepts identified at the workshop and feedback received through stakeholder outreach and engagement, five overarching R&D topics emerged that represent the National CISR R&D Priority Areas.

The five Priority Areas support the vision and objectives of this Plan and are intended to enable the development of both evolutionary and transformative approaches to enhancing the security and resilience of critical infrastructure systems and the goods and services they provide. This Plan and the R&D Priority Areas described in this section provide general guidance and flexibility to support the development and adoption of innovative R&D solutions for CISR. The entire critical infrastructure community should consider the National CISR R&D Priority Areas as potential focus areas for ongoing planning for CISR risk management and investment decisions. Individual critical infrastructure stakeholders should pursue these Priority Areas as appropriate to their unique circumstances, risks, and operating environments. Protection of privacy and civil liberties remains a key policy imperative in advancing the CISR R&D Priority Areas and the critical infrastructure community must apply robust safeguards accordingly.

Each of the five Priority Areas is discussed in more detail below, including a description of more specific examples of priorities within each area and potential supporting activities to advance the Priority Areas.

The National Priority Areas for CISR R&D are:

A. Develop the foundational understanding of critical infrastructure systems and systems dynamics

B. Develop integrated and scalable risk assessment and management approaches

C. Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure

D. Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action

E. Build a crosscutting culture of CISR R&D collaboration.

Priority Areas A, B, C and D are intended to follow a logical progression from the creation of a usable system-of-systems perspective across the critical infrastructure sectors and the subsequent identification of complementary analytical approaches to risk assessment and risk management (Priority Area B). Risk management strategies can then be translated into capabilities (Priority Area C) that can be integrated (Priority Area D) in support of the foundational systems understanding described in Priority Area A. Priority Area E represents a core enabling activity to promote the partnerships necessary for the successful advancement of the other Priority Areas. The numbering convention within each Priority Area is provided as a means to organize and reference the specific examples of priorities and potential supporting activities. It does not represent a rank ordering of the items listed.

A. Develop the Foundational Understanding of Critical Infrastructure Systems and Systems Dynamics

The critical infrastructure community needs to improve the foundational knowledge and understanding in a number of pivotal areas to support future advances in technologies and approaches for CISR. Due to the complexity of many critical infrastructure systems, empirical studies are often relied upon to establish principles or specifications for risk management or response activities. While these approaches have helped to mitigate known threats and hazards, the absence of comprehensive foundational understanding has limited their adaptive capacity in response to emerging and evolving threats and hazards, both episodic and lasting. A holistic understanding of the increasingly distributed, complex, and richly connected critical infrastructure environment has the potential to enable innovation in support of both evolutionary and transformative approaches. Areas of interest include the integrity, sustainability, reliability, and vulnerabilities of systems and system-of-systems architectures; the design and control of ICT systems; future diagnostic and real-time situational awareness capabilities; and the role of human factors in systems security and resilience.

The interdependencies that exist within and among infrastructure systems continue to grow in number and complexity and complicate the understanding of propagating system responses and cascading effects. While interdependencies are generally more readily understood at the individual asset level, there is a need for improved understanding of interdependencies at a systems level and on a broader, national scale, to include the potential strategic impacts that extend across sectors, regions, and international boundaries. To address this need, foundational research should focus on critical infrastructure systems architectures, infrastructure dynamics, and human/societal factors. A deeper understanding of infrastructure system dynamics and the linkages across domains will provide valuable insights into making critical infrastructure systems more secure and resilient. Enhanced measurement and predictive capabilities that incorporate human behaviors and responses can improve system operations and resilience.

A.1. Develop a foundational understanding of critical infrastructure systems, systems dynamics, and the relationships underlying interdependencies and cascading effects (including strategic, national-level effects)

A.1.1: Develop avenues of foundational science research, including structural/dynamic attributes, effects of human factors, and linkages to natural systems, to support enhanced security, resilience, and continuity of operations.

A.1.2: Develop a R&D roadmap for acquiring an integrated understanding of infrastructure systems—technological, physical, and natural—to include interdependencies and cascading effects.

A.1.3: Develop adaptive frameworks supporting integrated critical infrastructure and ICT infrastructure.

B. Develop Integrated and Scalable Risk Assessment and Management Approaches

Risk assessment is an essential component to strengthening the security and resilience of critical infrastructure. Risk assessment methodologies are designed to identify threats, assess vulnerabilities, and evaluate the consequences to assets, systems, and networks. However, risk assessment methodologies vary, in part, based on the system boundaries employed, the intended audience, and the applicable scale/level of assessment.

Many sectors have developed risk assessment and management approaches that are used to identify and manage risks at the organizational, community, or asset level. Some approaches are designed to focus narrowly on specific elements of interest and their corresponding level of detail to minimize the system definition requirements. These approaches often do not incorporate all relevant linkages and system dynamics, such as sector interdependencies, cybersecurity risk factors, spatial and temporal considerations, or the risk assessment and management strategies used by other entities. Where possible and appropriate, risk assessment methodologies should extend to secondary or tertiary effects and beyond, to capture the range of consequences associated with disruptions to the primary asset or system of interest. New, integrated risk methodologies should enable the explicit inclusion of these externalities that have potential to significantly alter the risk profile, leveraging knowledge gained through systems integration and data sharing across sectors and domains.

The development of integrated risk methodologies must consider the limitations associated with current assessment approaches. Among these limitations is the ability of methodologies to address extremely low-probability, high-consequence events. Innovative risk management frameworks are needed to support risk measurement and quantification approaches that produce outcomes comparable to other contemporary, probability-based risk methods.

While available assessment methodologies have been useful in supporting risk-informed decisions, additional work is needed to develop analytic tools and methods that foster appropriately integrated situational awareness to assist in making more deliberate, informed, and complex decisions. These tools and methods should be part of a larger framework to support complementary risk management decisions among a variety of stakeholders, including at the organizational, community, sector, and national levels.

In support of community interests, risk methodologies should emphasize ease of use, incorporating data sources and analytical approaches that can be readily applied at the local planning level. Risk methodologies should integrate best practices for identifying critical assets and business processes, and their associated risks, in developing and prioritizing risk management options.

Risk assessment methodologies should incorporate the effects that resilient designs and materials, response and recovery plans, resilient business processes, and human factors have on risk. Methodologies also should tie risk assessment outcomes with their primary drivers, allowing actions to be tailored to those specific areas with the highest influence on the outcomes.

B.1. Develop and field integrated risk assessment methodologies across the critical infrastructure community

B.1.1: Identify and characterize cyber and physical, cross-domain, economic, behavioral, societal, and environmental factors (and related data sets) that should be considered in fully integrated risk tools and in strategic decision-making.

B.1.2: Develop an integrated system-of-systems approach to risk assessment and risk management to include external/cross-domain factors and characteristics.

B.1.3: Develop verifiable and validated analytics for use in risk assessment methodologies and develop standards of practice for their application.

B.2. Develop the technical basis and analytical tools needed to incorporate dependencies and interdependencies into risk assessment and risk management methodologies

B.2.1: Identify and characterize dependency and interdependency dynamics for inclusion in risk assessment methodologies, appropriate to scale.

B.2.2: Develop verifiable and validated applied techniques for use in cross-domain risk assessment and develop standards of practice for their application.

B.3. Develop and disseminate best practices and methodologies for risk assessment and risk management

B.3.1: Develop methods to link essential community functions to the critical infrastructure systems that provide enabling services to build a systems understanding of community-wide functions that supports prospective risk management and response strategies.

B.3.2: Promulgate multi-attribute decision support approaches for identifying and prioritizing CISR investments at the community, regional, and national levels.

B.3.3: Identify standards of practice and functional requirements to support the expanded use of risk methodologies for cyber and physical systems and response planning.

C. Develop Integrated and Proactive Capabilities, Technologies, and Methods to Support Secure and Resilient Infrastructure

The development and deployment of secure and resilient technologies is essential to enhancing infrastructure security and resilience. New secure and resilient technologies will need to incorporate factors ranging from foundational research to implementation considerations. A proactive, prospective approach to CISR includes the development of capabilities that enable systems to anticipate disruptions and quickly adapt, providing human operators with actionable alternatives to minimize or avert system compromise. Consistent with PPD-21, a holistic approach to CISR should integrate a wide range of physical and cyber considerations.

Secure and resilient technologies should be driven and enabled by adaptive, application-specific policies, regulations, and strategies, and supported by well-trained and informed individuals. The human element is central to CISR; the people who operate and maintain infrastructure systems must possess the skills and tools necessary to perform their jobs optimally. Social and behavioral research can help identify ways to enable humans to act and respond more securely and effectively.

The continued use of new regenerative and sustainable materials has the potential to lower maintenance costs while improving system performance and resilience. The expanded use of standardized, interoperable components can eliminate design constraints and inefficiencies, and enable rapid retrofit and recovery capabilities. Green infrastructure (e.g., using strategically located natural barriers) can help to protect communities from natural disasters, are naturally regenerative and sustainable, and require minimal maintenance.

Other strategies—including real-time diagnostic and anomaly detection capabilities—can enable dramatic improvements in situational awareness and response. In addition, advances in multi-tiered cybersecurity approaches and policies for people and organizations, hardware systems, software/data, and application services will further strengthen ICT systems against cyber-related incidents.

Through improved data acquisition, real-time situational awareness and surveillance, and threat identification, critical infrastructure systems can respond to threats and incorporate protective countermeasures that deploy with or without human intervention. Critical infrastructure owners and operators can implement properly tested and configured countermeasures to defeat or mitigate a threat, or gracefully degrade service under duress, improving system resilience and limiting the possibility of cascading failures. System learning derived from operational data and exercises can help identify adaptive strategies for CISR. Advances in inherently secure and resilient infrastructure can be made over the short- and medium-term timeframes through focused and coordinated R&D programs.

C.1. Characterize the predictive and proactive capabilities needed to forecast and prepare for threats and hazards

C.1.1: Identify specific areas or technologies with the potential to enable predictive and proactive or regenerative processes.

C.1.2: Leverage advances in sensor technologies, data sciences, and analytics to develop improved all-hazard predictive capabilities for cyber and physical systems.

C.2. Identify policies, governance structures, and regulations that support and enable timely and responsive actions

C.2.1: Identify and characterize enabling policies, structures, and regulations that support action to execute programs and drive resilient outcomes.

C.2.2: Develop standards of practice to harmonize existing policies, regulations, and codes and standards to enhance community resilience.

C.3. Develop capabilities to identify and rapidly integrate new technologies and respond to the evolving threat environment

C.3.1: Develop capabilities to analyze new technologies and evolving threats, characterize their effects, and disseminate actionable guidance and recommendations.

C.3.2: Identify and transfer the range of new technologies required for the enhanced security and resilience of networked critical infrastructure systems and their transition to practice.

C.3.3: Develop new materials, material guides, and design and manufacturing processes leveraging novel approaches and linkages to eliminate or reduce design and retrofit constraints.

C.3.4: Leverage complexity sciences to characterize the challenges, implications, and opportunities presented by the increasingly distributed, complex, and richly connected critical infrastructure environment.

C.3.5: Promote the robust, effective design and construction of cyber-physical systems and infrastructure.

D. Harness the Power of Data Sciences to Create Unified, Integrated Situational Awareness and to Understand Consequences of Action

Recent advances in data sciences, combined with increasingly pervasive sources of information, are transforming how operational data can be used to create situational awareness and enable informed resilience decision-making. More accurate analyses, based on the timely acquisition of quality data, can result in reduced risk, greater operational efficiencies, and decreases in cost. Combined with advanced modeling and simulation capabilities, the decision maker can gain valuable insights in current operational status and increase the accuracy of predicted future outcomes and consequences of action. Challenges in creating a unified, integrated situational awareness capability include securing data required for the analysis, ensuring the timeliness and quality of the data acquisition, and applying appropriate analytics to assess and integrate the data to support decision-making. A robust evaluation process for the analytical tools will result in more meaningful products for dissemination and use in the decision-making process.

To enable integrated situational awareness across sectors and domains, sharing results also requires interoperability standards and frameworks that ensure the proper interpretation and integration of data into domain-specific analysis tools and models. Situational awareness capabilities also should include surveillance, tracking, and other technologies to increase awareness and reduce exposure to threats in real and virtual environments. With advances in surveillance technologies, new capabilities are available to identify suspicious activities and system anomalies, and to track their movements through systems.

At the same time, the use of surveillance, analysis, and predictive capabilities may present potential risks for individual privacy and civil liberties. The impact of such capabilities should be considered so that such risks can be mitigated to the greatest extent possible. Information sharing within the critical infrastructure community can and must be done in a manner that respects privacy and civil liberties.

Predictive modeling and simulation tools should properly characterize the system under examination and document, where possible, measures of confidence in the data used and generated. Structured modeling and simulation capabilities can inform timely decision-making through improved understanding of critical infrastructure relationships and their effects across multiple domains. Predictive analysis capabilities must be scalable and include an understanding of the emergent structural characteristics and properties of the increasingly expansive, complex, and interconnected critical infrastructure environment.

D.1. Investigate the potential for increased situational awareness from data sciences and the increased use of sensor networks, augmented by networked intelligent systems and analysis

D.1.1: Characterize the architectures and requirements of integrated data acquisition networks and intelligent systems for enhanced situational awareness.

D.1.2: Establish criteria and standards for broad-scale data acquisition and establish ontology and topology frameworks for sharing data across domains.

D.1.3: Investigate privacy, legal, or regulatory factors associated with broad-scale information sharing from point sources and across domains.

D.2. Develop the data sciences to support unified, integrated situational awareness

D.2.1: Identify future R&D activities in cross-sector data analytics to support CISR.

D.2.2: Catalog and disseminate information on analytical tools and data currently available for CISR.

D.3. Develop modeling and analysis capabilities that properly characterize critical infrastructure systems and integrate cross-sector dynamics

D.3.1: Identify common capabilities for the extensible and scalable integration of modeling tools with varying granularity and timescales—from nano to macro scales.

D.3.2: Develop a R&D roadmap for future CISR modeling and analysis capabilities.

D.3.3: Define public and private sector usability requirements for modeling and analysis capabilities at the State, regional, and local levels.

E. Build a Crosscutting Culture of CISR R&D Collaboration

A national effort to advance the CISR R&D Priority Areas requires integrated action across the critical infrastructure community. The many different stakeholder organizations involved in CISR R&D must join together through a common vision and unity of effort supported by awareness, information sharing, and collaborative action. This includes coordinating with international partners, as appropriate, to identify and pursue shared CISR R&D needs.

Significant and groundbreaking CISR R&D will require changes in how the critical infrastructure community plans, conducts, and executes R&D programs and shares results across sectors and domains for broad implementation by practitioners. Current collaboration is widespread and productive, but is often confined to teams of researchers with similar expertise in theory, computation, or practice. An integrated multidisciplinary and interdisciplinary approach can accelerate R&D progress as results from each perspective inform the work of the others, enhancing communication across disciplines, avoiding delays and missteps, and enabling sustainable and scalable approaches to CISR.

The ultimate goal of CISR R&D is the efficient and effective transition of new and innovative capabilities and technologies into practice. Common crosscutting capabilities can be developed that collectively support the goals of the larger community. Critical infrastructure owners and operators can develop a common understanding of future operational requirements and communicate those needs to research teams throughout the development process. This engagement helps guide the development of R&D solutions to operational challenges and eases the integration of new technologies and approaches into current systems, processes, and procedures.

Training and education programs should integrate cross-sector and cross-domain perspectives to ensure that individuals, teams, and organizations share a common understanding of risk and interdependencies. Leadership responsibilities across the critical infrastructure enterprise include promoting sector, organizational, and community commitments to enhancing security and resilience and ensuring that supporting activities continue over time. Critical infrastructure stakeholders should incorporate key elements of this Plan, including the National CISR R&D Priority Areas, into their training and education programs, as appropriate to their risk and operating environments.

E.1. Encourage broad initiatives to develop a crosscutting culture of CISR R&D collaboration

E.1.1: Promote collaboration and information sharing in R&D areas offering significant, sustainable, and scalable approaches to CISR.

E.1.2: Encourage the development of training and education curricula focused on cross-disciplinary approaches that support system, organizational, domain, and cross-domain security and resilience.

E.1.3: Develop a crosscutting culture and skills to examine and communicate the operational complexity and interdependencies of critical infrastructure, through integrated multidisciplinary and interdisciplinary teams.

E.1.4: Develop technologies, codes, and standards of practice supporting the justification for, and encouraging the adoption of, new and existing security and resilience approaches.

5. Advancing the National CISR R&D Priority Areas

This section discusses the importance of partnership among critical infrastructure stakeholders as the foundation of CISR R&D and describes related collaborative activities. Because no single sector or entity—public or private—has all the capabilities, capacity, and authority necessary to independently advance the National CISR R&D Priority Areas, the critical infrastructure community must work collectively to define and pursue requirements and goals for future CISR R&D programs. Each group and partner has different roles and responsibilities, operating environments, and perspectives that contribute to R&D activities in support of sector and national security and resilience.

> *"To be most effective, Federal departments and agencies, critical infrastructure owners and operators, and SLTT entities must work collaboratively on R&D efforts to proactively manage all-hazard risks that could have a debilitating impact…"*
>
> Source: Presidential Policy Directive 21
>
> *"We must partner with industry in research and development efforts to reduce known vulnerabilities that have proved difficult or expensive to address—particularly in cyberspace and critical infrastructure—and to mitigate consequences of disruption or intrusion."*
>
> Source: 2014 Quadrennial Homeland Security Review

The coordinated pursuit of the National CISR R&D Priority Areas and the timely transition of R&D solutions into practice are dependent on leveraging and strengthening existing partnerships and fostering new relationships where needed. Significant investments in R&D are planned and executed across the CISR community and existing critical infrastructure partnership structures can provide an effective vehicle for cross-sector R&D coordination. Such partnerships exist within and across the sectors and can be local, regional, or national in scope.

Other venues and partnerships offer additional opportunities to engage the critical infrastructure community in CISR R&D activities. These venues include conferences, workshops, and meetings organized by stakeholder groups, sectors, and private entities. The Sector Coordinating Councils, composed of private sector owners and operators within each critical infrastructure sector, serve as principal entry points for the government to collaborate with the sectors on CISR R&D efforts. Building communities of practice will facilitate the development of innovative approaches and technologies. Support for transitioning R&D solutions to the critical infrastructure community and other users may include a range of stakeholders and other organizations or legal entities.

Information Sharing

As described in Section 4, CISR R&D requires the critical infrastructure community to plan and execute R&D programs collaboratively and share results across sectors and domains. Effective information sharing is a core element of successful partnership and contributes directly to an open and supportive environment. The critical infrastructure community should share information, including risk management strategies,

approaches, and lessons learned. Information sharing also supports efforts to incorporate existing knowledge into tools and technologies that can be more easily transitioned and integrated into practice.

Sharing lessons learned and best practices can help partners identify the actions needed to invest in, plan, and implement R&D activities. The sharing of risk information and methodologies will strengthen the collective capabilities of critical infrastructure owners and operators to assess risk, leading to more informed investment decisions.

Policy, Legal, and Regulatory Environment

Policy, legal, and regulatory mechanisms can be leveraged to remove or reduce barriers to successful CISR R&D, creating an environment more conducive to innovation and partnership. Codes and standards can create efficiencies, reduce uncertainty, and accelerate technology acceptance and adoption to advance CISR across all sectors. Specifications, recommended practices, classifications, test methods, and guides that promote security and resilience must be continually updated to address the evolving risk and operating environments.

In many sectors, standards development organizations provide the mechanisms to develop codes and standards specific to their industry. Voluntary consensus standards, developed and approved by interested stakeholder/industry groups in standards-setting organizations, and regulations mandated by law, provide specific guidance and requirements on the design, construction, maintenance, security, and safe operation of many critical infrastructure systems and assets. Standards development organizations should encourage and facilitate the development of new codes and standards for CISR as risks warrant. For sectors dominated by physical assets, existing standards and regulations address security, resilience, aging, and other factors. The critical infrastructure community should continue to evolve these standards to support efficient mitigation of changing threats and hazards.

Standard guides and practices also may quantify performance-based requirements and create financial incentives that drive adoption of desirable features and behaviors. These types of standards define frameworks and accepted methodologies for assessing performance. There is a need for greater alignment and harmonization among the many, varied industry standards, regulatory frameworks, and national policies governing the critical infrastructure sectors.[5]

Design and Execution of CISR R&D Programs

This National CISR R&D Plan is intended to leverage the significant investments in high-quality R&D being planned and executed across the critical infrastructure community and to promote coordination across efforts and timeframes. Research programs cover the spectrum from foundational to applied research and operate over different time horizons. Much of this work is guided by collaborative research agendas that align research programs with organizational missions and community needs.

Integrated multidisciplinary R&D programs are widely recognized as being highly effective and results-oriented. By design, these programs strive to integrate a broad range of requirements and perspectives from different stakeholder groups in defining the program scope and outcomes, and guide program execution to ensure the outcomes meet the specified requirements and stakeholder needs.

[5] *Critical Infrastructure Security and Resilience National Research and Development Plan: Final Report and Recommendations*, National Infrastructure Advisory Council, November 14, 2014.

Measurement of Progress

The critical infrastructure community should develop and share reliable measures to evaluate the effectiveness of R&D activities in advancing the National CISR R&D Priority Areas identified in Section 4. This National CISR R&D Plan supports the development of metrics appropriate to the R&D environment, to demonstrate progress against the Priority Areas and to create a more explicit decision-making framework to implement programs that are results-oriented by design. Such metrics are intended to ensure that programs are effectively and efficiently managed and that resulting products meet user requirements and remain cost-effective from a development and application perspective. In support of NIPP 2013 Call to Action #2,[6] this Plan is also intended to inform sector-level planning, which should include the evaluation of sector contributions to advancing the National CISR R&D Priority Areas.

[6] "The Sector-Specific Plans (SSPs) will … guide development of appropriate metrics and targets to measure progress toward the national goals and priorities, as well as other sector-specific priorities." NIPP 2013

6. Conclusion and Path Forward

This National CISR R&D Plan is intended to strengthen national CISR R&D efforts and outcomes, through collaboration, partnership, and information sharing across the critical infrastructure community.

This Plan responds to the tasking in PPD-21, to provide to the President a National CISR R&D Plan that identifies priorities and guides R&D requirements and investments to support the security and resilience of the Nation's critical infrastructure. Subsequent releases will continue to be developed in collaboration with the critical infrastructure community and issued every four years, with interim updates as needed.

To support implementation of this Plan, critical infrastructure stakeholders are encouraged to:

- Document and share current R&D activities and their transition to use;
- Align sector R&D planning with the National CISR R&D Priority Areas;
- Work with all partners and stakeholders—within and across sectors and levels of government—to share information and ensure coordination and integration of efforts to advance the National CISR R&D Priority Areas, including collaboration with international partners;
- Work collaboratively to plan and execute new and future R&D activities;
- Identify legal and other barriers that may impede Plan implementation; and
- Develop and implement effective measures to demonstrate progress against the National CISR R&D Priority Areas.

Federal Governance Structure and Next Steps

As stated in PPD-21, "The Secretary of Homeland Security, in coordination with the Office of Science and Technology Policy (OSTP), the SSAs, Department of Commerce, and other Federal departments and agencies, shall provide input to align those Federal and federally funded R&D activities that seek to strengthen the security and resilience of the Nation's critical infrastructure." To facilitate this interagency coordination, the Federal CISR R&D community will be convened under the National Science and Technology Council (NSTC) structure through the creation of a subcommittee. The subcommittee will draw on critical infrastructure subject matter experts and thought leaders with national perspective and the skills to formulate critical infrastructure research requirements to meet future needs.

Within 60 days of creation of the subcommittee, DHS will initiate the development of a National CISR R&D Plan Implementation Roadmap, with input from interagency stakeholders, outlining Federal steps to implement the Plan and identifying key deliverables for aligning Federal R&D activities. The Implementation Roadmap also will describe how DHS will coordinate with CISR stakeholders to develop annual performance metrics by National CISR R&D Priority Area, to provide a means of tracking the alignment of R&D activities that strengthen CISR. The first annual metrics will be developed within six months of issuance of the Implementation Roadmap.

Implementation of the CISR R&D Plan will continue to support other national efforts to enhance security and resilience, such as identifying R&D requirements for building, sustaining, and delivering the core capabilities to achieve the National Preparedness Goal and efforts to advance the Joint National Priorities established through NIPP 2013 Call to Action #1. The Implementation Roadmap will leverage existing mechanisms wherever possible, to align with and inform current reporting efforts, such as the Critical Infrastructure National Annual Report and the National Preparedness Report.

Stakeholder Outreach and Engagement

Effective implementation of the National CISR R&D Plan will require outreach and engagement to ensure the inclusion of a broad range of perspectives across the critical infrastructure community. CISR R&D stakeholders can leverage a range of existing mechanisms, including regular updates and opportunities for discussion at meetings, research symposia, and national conferences and workshops, and the use of webinars and online forums. DHS will launch a dialogue through S&T's National Conversation on Homeland Security Technology[7] to solicit ideas and incentivize innovative solutions to strengthen CISR.

DHS will facilitate additional opportunities for continued engagement, including direct outreach to key sector, SLTT, and regional groups, and ongoing coordination through existing partnership structures. Federal departments and agencies, working through the SSAs and the Federal Senior Leadership Council as appropriate, should share information on CISR R&D topics and Priority Area progress with the critical infrastructure community, to ensure broad awareness and to support a coordinated national approach to advancing the National CISR R&D Priority Areas.

This Plan recognizes the global and interconnected nature of critical infrastructure and supports the PPD-21 requirement that the Federal Government "engage with international partners to strengthen the security and resilience of domestic critical infrastructure and critical infrastructure located outside of the United States on which the Nation depends." The Implementation Strategy will describe how critical infrastructure stakeholders should work together to share information, implement existing agreements affecting CISR R&D, and enhance understanding of cross-border interdependencies of critical infrastructure.

As stated in PPD-21, "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." Focused and integrated R&D programs developed through public-private collaboration will drive the discovery and innovation necessary to strengthen the security and resilience of the Nation's critical infrastructure, now and into the future.

[7] See http://www.dhs.gov/science-and-technology/join-conversation.

Acronyms

CISR Critical Infrastructure Security and Resilience

DHS Department of Homeland Security

EO Executive Order

ICT Information and Communications Technologies

NIPP National Infrastructure Protection Plan

PPD Presidential Policy Directive

R&D Research and Development

S&T Science and Technology Directorate of the Department of Homeland Security

SLTT State, Local, Tribal, and Territorial

SNRA Strategic National Risk Assessment

SSA Sector-Specific Agency

SSP Sector-Specific Plan

Glossary of Terms

Many of the definitions in this Glossary are derived from language enacted in Federal laws and/or included in national plans and Presidential directives, including the USA PATRIOT Act of 2001; NIPP 2013; 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. For purposes of the National CISR R&D Plan, these definitions apply.

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)

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 and other negative outcomes to society. (Source: Adapted from DHS Lexicon, 2010)

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Source: §1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e))

Critical Infrastructure Community. Critical infrastructure owners and operators, both public and private; Federal departments and agencies; regional entities; 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 and/or promoting practices and ideas for doing so. (Source: NIPP 2013)

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: NIPP 2013)

Dependency. The one-directional reliance of an infrastructure 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: NIPP 2013)

Executive Order 13636. Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity framework; and promote and incentivize the adoption of strong cybersecurity practices. (Source: EO 13636, February 2013)

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)

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

Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole; consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (Source: DHS Lexicon, 2010)

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)

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 to perform a function. (Source: NIPP 2013)

Partnership. Close cooperation between parties having common interests in achieving a shared vision. (Source: NIPP 2013)

Presidential Policy Directive 8 (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; 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)

Presidential Policy Directive 21 (PPD-21). Aims to clarify roles and responsibilities across the Federal Government and establish a more effective partnership with owners and operators and SLTT entities to enhance the security and resilience of critical infrastructure. (Source: PPD-21, 2013)

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

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)

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; the National Plan addresses 16 critical infrastructure sectors, as identified in PPD-21. (Source: NIPP 2013)

Sector-Specific Agency (SSA). A Federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (Source: PPD-21, 2013)

Sector-Specific Plans (SSP). Planning documents that complement and tailor application of the National Plan to the specific characteristics and risk landscape of each critical infrastructure sector; developed by the SSAs in close collaboration with the SCCs and other sector partners. (Source: NIPP 2013)

Secure/Security. 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. (Source: PPD-21, 2013)

System. Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose. (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)

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

Homeland
Security