Timing — ?

Critical Infrastructure Protection

NSC cont. cybersec - Admin
DHS other agencies

Purpose

To strengthen and maintain secure, functioning, and resilient critical infrastructure by updating United States policy to promote a national unity of effort for critical infrastructure protection.

Introduction

Critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, systems, and functions – that are vital to the Nation's safety, prosperity, well-being, and public confidence.

This directive updates national policy, revising the Federal government's approach to critical infrastructure protection and resilience, recognizing this endeavor as a shared responsibility across Federal, State, local, tribal and territorial governments, and owners and operators of critical infrastructure. Through this directive it is also intended that by refining and clarifying the Federal government architecture, public and private access points will be more clear and facilitate enhanced collaboration. In addition, the Federal government has a responsibility to protect its own critical infrastructure and mission essential functions, and to organize itself to enable effective partnerships with and add value to the protection and resilience efforts of critical infrastructure owners and operators.

The Nation's critical infrastructures are complex, including distributed networks; diverse organizational structures and operating models; interdependent functions and systems in both the physical and cyber space; and governance constructs that involve multi-leveled authorities, responsibilities, and regulations. Public and private owners and operators of critical infrastructure (herein referenced as "critical infrastructure owners and operators") are best positioned to manage risks to their individual operations and assets, and to determine the optimal strategies to protect them and make them more resilient. Because of the interdependent nature of essential services underpinning American society, it is also the case that there is a need for a level playing field with respect to security to minimize weak links across the enterprise. It is therefore essential that a mutually beneficial arrangement for public-private collaboration be further developed, including collective efforts to address threats and known and emerging vulnerabilities to safeguard the provision of essential services necessary to support the well being of the American people.

Policy

It is the policy of the United States to strengthen our capabilities and mechanisms to enhance the protection and resilience of physical and cyber aspects of the Nation's critical infrastructure.

The Federal government shall work with critical infrastructure owners and operators and State, Local, Tribal, and Territorial (SLTT) entities to take proactive steps to manage risk and protect the Nation's critical infrastructure against all hazards that could have a debilitating impact on security, economic stability, public health and safety, or any combination thereof. These efforts shall aim to reduce vulnerabilities, deter threats, minimize consequences, strengthen resilience, and support timely response and recovery decisions and actions for critical infrastructure in the event of a deliberate attack, natural disaster, or other emergency.

Through proactive international engagement, the Federal government shall also seek to strengthen the protection and resilience of critical infrastructure, including infrastructure located outside of the United States on which the Nation depends.

The Nation's critical infrastructure is interconnected and interdependent, and United States policy shall address the protection and resilience of physical and cyber assets in an integrated, holistic manner. This policy also identifies the Energy Sector and the Communications Sector as uniquely critical, with key dependencies that cut across all other critical infrastructure sectors. Dependence on the Energy and Communications Sectors shall be identified and included in protection and mitigation efforts across all sectors.

Three strategic imperatives shall drive the Federal approach:

1) Revise the United States Government architecture to enhance the protection and resilience of critical infrastructure;
2) Develop and implement an information exchange framework to enable effective collaboration; and
3) Implement a physical infrastructure and cyber integration and analysis function to provide a Nation-wide common operating picture for critical infrastructure.

All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal critical infrastructure, to include mission essential functions. Such infrastructure shall be reflected in the plans and execution of the requirements in National Security Presidential Directive-51/Homeland Security Presidential Directive-20 - *National Continuity Policy*.

Federal departments and agencies shall implement this directive in a manner consistent with applicable law, Presidential directives, and Federal regulations, including those protecting civil rights and civil liberties. In addition, Federal departments and agencies shall protect all information associated with carrying out this directive consistent with the Homeland Security Act of 2002 and other applicable legal authorities and policies.

Roles and Responsibilities

The effective implementation of this policy requires strategic guidance from the Secretary of Homeland Security, expertise and day-to-day engagement from the Sector-Specific Agencies, specialized or support functions from other Federal departments and agencies, and strong collaboration with critical infrastructure owners and operators and SLTT entities. While the roles and responsibilities identified in this policy are directed at Federal departments and agencies, effective partnerships with critical infrastructure owners and operators and SLTT entities are imperative to protect the Nation's critical infrastructure. What is intended is a layered and distributed national architecture with strategic, overarching guidance to establish a national plan which sets a common compass heading, and day-to-day collaboration and coordination with and through Sector-Specific Agencies.

Secretary of Homeland Security

The Secretary of Homeland Security shall serve as the strategic coordinator for the national effort to enhance the protection and resilience of the critical infrastructure of the United States. Pursuant to the Homeland Security Act of 2002, the Secretary of Homeland Security evaluates national capabilities, opportunities, and challenges against the risk landscape, vulnerabilities, and threats to critical infrastructure sectors. This analysis shall be used to develop strategic guidance to manage risk, measure effectiveness, and strengthen the Nation's protection and resilience posture for critical infrastructure.

The Secretary of Homeland Security's role includes coordination with Sector-Specific Agencies and relevant Federal departments and agencies, and sets overarching guidance for collaboration with critical infrastructure owners and operators, independent and regulatory agencies, and SLTT entities, identifying strategic-level protection and resilience functions that are necessary for effective public-private engagement with all critical infrastructure sectors.[1] The Secretary of Homeland Security also has the responsibility to establish metrics to evaluate progress toward reducing known and emerging vulnerabilities, including a feedback mechanism to foster Federal accountability.

[1] An example is the ability to exchange information at the SECRET level.

Sector-Specific Agencies

Each critical infrastructure sector has unique characteristics, operating models, and risk profiles that benefit from an identified lead that has institutional knowledge and expertise about the sector. Recognizing existing statutory and/or regulatory authorities of specific Federal departments and agencies, and leveraging existing sector familiarity and relationships, Sector-Specific Agencies (SSAs) shall carry out the following roles and responsibilities for their respective sectors:

1) Recognize their role and contribution as part of the broader national framework for the protection and resilience of all critical infrastructure sectors, including being responsive to strategic guidance issued by the Secretary of Homeland Security, as the national critical infrastructure protection strategic coordinator;
2) Facilitate the implementation of national policies and strategic-level protection and resilience functions for the critical infrastructure sectors as it relates to this directive;
3) Serve as a day-to-day Federal interface for the dynamic prioritization and coordination of sector-specific activities to include, but not limited to, protection, situational awareness, planning, preparedness activities, risk assessments, sector and national reporting, engagement, and exercises related to critical infrastructure protection and resilience;
4) Facilitate the integration of physical and cyber critical infrastructure protection within the sector;
5) Lead or support non-cyber incident management activities consistent with statutory authority, Presidential Policy Directive (PPD)-8: National Preparedness implementation, and other appropriate directives or regulations;
6) In the event of a national or significant cyber incident, the SSAs and critical infrastructure owners and operators shall work through the established cyber protocols identified by the Secretary of Homeland Security in the National Cyber Incident Response Plan (NCIRP), or its successor;
7) Provide support and/or timely information to the national critical infrastructure coordination centers (identified below in Strategic Imperative #1); and
8) Coordinate with DHS and other relevant Federal departments and agencies and collaborate with critical infrastructure owners and operators, independent and regulatory agencies, and SLTT entities, to implement this directive.

Additional Federal Responsibilities

Additional specialized or support functions related to critical infrastructure protection and resilience shall be carried out by, or along with, other Federal departments and agencies and regulatory agencies, including:

1) The Department of State, together with the Department of Homeland Security (DHS), SSAs, and other Federal departments and agencies, shall engage foreign governments and international organizations to strengthen the protection and resilience of critical infrastructure located outside of the United States, particularly foreign-based infrastructure creating dependencies on partner nation states, and to facilitate the overall exchange of best practices and lessons learned for protecting and promoting the resilience of critical infrastructure on which the Nation depends;
2) The Department of Defense (DOD) is responsible for planning, coordinating, integrating, synchronizing, and directing activities to operate and defend DOD critical infrastructure and information networks.
3) The Department of Justice (DOJ), including the Federal Bureau of Investigation, plays a critical role in reducing domestic terrorist threats and by law, investigates and prosecutes actual or attempted terrorist or criminal attacks on, sabotage of, or disruptions of critical infrastructure and key resources. In addition, recognizing their shared responsibilities for threat reduction, the Attorney General and the Secretary of Homeland Security shall collaborate to safeguard the protection and resilience of critical infrastructure, where the PPD-1[2] process shall be used to resolve disputes.
4) The Department of Interior, in collaboration with the SSA for the Government Facilities Sector, shall identify, prioritize, and coordinate the protection and resilience of national monuments and icons and incorporate all-hazards protective measures to reduce risk to these critical assets, while also promoting the use and enjoyment of this infrastructure;
5) The Department of Commerce (DOC), in collaboration with DHS, will engage private sector, research, academic, and government organizations to improve supply chain security for technology and tools related to cyber-based systems, and promote the development of other critical infrastructure efforts to enable the timely availability of industrial products, materials, and services to meet homeland security requirements;
6) The Office of the Director of National Intelligence (ODNI), DOD, and DHS shall use applicable authorities and coordination mechanisms to provide 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 shall be 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;
7) The General Services Administration shall provide government-wide contracts ensuring that all private sector services, supplies, and personnel provided in conjunction with

[2] Presidential Policy Directive-1 is the Organization of the National Security Council System.

critical infrastructure systems include a description of and permit an audit of all measures associated with the protection and resilience of critical infrastructure; and

8) The Nuclear Regulatory Commission (NRC) shall oversee 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 shall continue to collaborate with DHS, the Department of Energy, the Environmental Protection Agency, and other Federal departments and agencies, as appropriate, on strengthening critical infrastructure protection and resilience.

Three Strategic Imperatives

1) Revise the United States Government Architecture to Enhance the Protection and Resilience of Critical Infrastructure

Over the past decade, lessons learned regarding the protection of critical infrastructure and an understanding of critical infrastructure sector interdependencies has evolved and will continue to do so. During this time, new programs and entities have been created to address specific infrastructure issues; protection priorities have shifted and expanded; and threats have become increasingly dynamic. As a result, the Federal architecture shall be revised and streamlined to reinforce baseline capabilities that will reflect this evolution of knowledge, and clearly define programs and access points to facilitate collaboration and information exchange between the United States Government and owners and operators of critical infrastructure and SLTT entities.

As part of this revised architecture, there shall be two coordination centers under the purview of DHS - one for physical infrastructure and another for cyber – which shall function in an integrated manner and serve as an overall clearinghouse and central access point for interaction with SLTT and private industry. Together, these centers shall be the Federal government's focal point for situational awareness and actionable information to protect the physical and cyber aspects of critical infrastructures. While operational and technical differences exist between physical and cyber space, physical and cyber elements of critical infrastructures and their vulnerabilities are inextricably linked. These critical infrastructure elements must be at once considered independently, but also viewed holistically. In addition, an integration and analysis function shall be implemented at the nexus of these two centers to support the necessary linkages, including the need for a common operating picture. This function is further developed in Strategic Imperative #3.

The success of these independent but linked centers, including the integration and analysis function, is dependent on the quality and timeliness of the information they receive from the SSAs and other Federal departments and agencies, as well as from critical infrastructure owners and operators and SLTT entities. The intent is a value proposition for all, where these U.S. Government coordination centers are expected to provide information to all with a role and responsibility to protect and promote the resilience of the Nation's critical infrastructure.

In addition, there shall be an adaptable National Plan that leverages the revised Federal architecture and further strengthens the protection and resilience of critical infrastructure. This plan, which will supersede the current National Infrastructure Protection Plan (NIPP), shall include a risk management framework that will:

a. Inform action to secure critical infrastructure;
b. Identify methods to promulgate threat awareness;
c. set requirements for vulnerability and risk assessments;
d. Issue recommendations for specific protective measures relevant to the evolving threat landscape;
e. Initiate a risk-based process to identify, classify, and prioritize the Nation's critical infrastructure;
f. Establish linkages between physical and cyber critical infrastructure elements and options to strengthen their integration;
g. Facilitate streamlined collaboration and information sharing mechanisms;
h. Address interdependencies among critical infrastructure sectors; and
i. Promulgate strategic guidance and metrics for annual reports to Congress, as well as their alignment with PPD-8 deliverables.

While the national plan will establish physical and cyber linkages, the details of the cybersecurity roles, responsibilities, and protocols are defined in the NCIRP, or its successor.

2) <u>Develop and Implement an Information Exchange Framework to Enable Effective Collaboration</u>

Because the majority of the Nation's critical infrastructure is owned and operated by the private sector, efforts to strengthen and maintain secure, functioning, and resilient critical infrastructure requires effective and routine collaboration and information exchange between all levels of government and critical infrastructure owners and operators.

Effective collaboration mechanisms and information exchange protocols are essential to inform decisions and guide coordinated action; facilitate the timely exchange of threat and

vulnerability information as well as actionable protective action; support collaboration with and among critical infrastructure sectors; promote a common understanding of public and private entities; establish working relationships and operating standards prior to a crisis; coordinate security measures to create a level playing field across sectors; and facilitate an optimization of resources to advance our collective ability to act when a threat is present or an incident occurs.

Information exchange has been an evolving process within and across the critical infrastructure sectors and continued focus is necessary to address challenges due to the amount and types of information available, the number of entities that possess this information, and the ability to exchange the information. To address these challenges, an information exchange framework shall be developed that includes baseline information exchange mechanism requirements, access points within the sectors, and identified systems and processes to streamline the effort.

3) Implement a Physical Infrastructure and Cyber Integration and Analysis Function to provide a Nation-wide Common Operating Picture for Critical Infrastructure

The third strategic imperative builds on the first two and calls for the implementation of an integration and analysis function that supports the development of a near-real time Nation-wide common operating picture for critical infrastructure. This integration and analysis function, which sits at the intersection of the two coordination centers as identified in Strategic Imperative #1, shall include the capability to collate, assess, and integrate vulnerability information with threat streams and hazard information to:

a. Aid in managing risks to critical infrastructure;
b. Project interdependencies and cascading impacts;
c. Recommend protective measures; and
d. Support incident management and reconstitution of critical infrastructure.

This function shall integrate various sources of information to inform key decision points. In implementing this function, attention will be given to critical infrastructure's importance to the global supply chain; an assessment of the most critical infrastructure to protect given a particular threat or incident; and the identification of cascading effects if specific critical infrastructure is compromised and how it might impact national imperatives such as national security, economic stability, and/or public health or safety.

ODNI, DOD, DOJ, DHS, and other Federal departments and agencies with relevant intelligence have a critical role to play to inform this integration and analysis capability regarding the Nation's critical infrastructure. They shall provide intelligence on plans, capabilities, and

intentions of threat actors and provide support to the analysis at the intersection of threat and vulnerability to inform decisions and actions, subject to applicable laws and authorities.

Finally, with the implementation of a revised Federal architecture, effective collaboration mechanisms, an information exchange framework, and an integration and analysis function, DHS shall maintain and share as a common Federal service, a near-real time common operating picture for critical infrastructure that includes actionable information about imminent and emergency threats, significant emerging trends, and awareness of incidents that may impact critical infrastructure.

Innovation and Research and Development

The Secretary of Homeland Security, in coordination with the Office of Science and Technology Policy (OSTP), the SSAs, DOC, and other Federal departments and agencies, shall focus and align the Federal and Federally funded research and development (R&D) activities aimed to enhance the protection and resilience of the Nation's critical infrastructure, to include:

1) Promoting R&D to enable the secure and resilient design and construction of critical infrastructure and more secure accompanying cyber technology;
2) Enhancing modeling capabilities to determine potential impacts on critical infrastructure given an incident or threat scenario, as well as cascading effects to other sectors;
3) Facilitating initiatives to incentivize cybersecurity investments and the adoption of critical infrastructure design features that strengthen all hazards protection and resilience; and
4) Prioritizing efforts to support the strategic guidance issued by the Secretary of Homeland Security.

Implementation of the Directive

Implementation of this directive requires specific deliverables that support the three strategic imperatives:

1) Functional adjustments to elements of the DHS National Protection and Programs Directorate;
2) The development of a new National Plan, including an initial interim outline and a schedule for its development;
3) Evolution of sector coordination mechanisms;
4) Development of an Information Exchange Framework;
5) Demonstration of a near-real time common operating picture for physical and cyber critical infrastructure; and

6) A Critical Infrastructure Protection and Resilience R&D Plan.

1) Description of DHS Infrastructure Protection Architecture

Within 75 days of this directive, the Secretary of Homeland Security shall provide to me, via the Assistant to the President for Homeland Security and Counterterrorism, a description of functional adjustments made to DHS infrastructure protection programs, coordination centers, and associated capabilities to meet the requirements of this directive. The Secretary of Homeland Security shall make any necessary notifications to Congress as required under the Homeland Security Act of 2002 (as amended). Specifically, the deliverable shall:

1) Provide an updated description of the functions of the National Preparedness and Protection Programs Directorate and associated key capabilities, roles, and responsibilities.
2) Articulate strategic intent regarding the integration of effort among the physical and cyber centers called for in Strategic Imperative #1, which shall serve collectively as the focal point for physical and cyber aspects of critical infrastructure protection - including the coordination of cyber incident response per the NCIRP, or its successor - in collaboration with other Federal departments and agencies.
3) Identify the responsibilities, location, and array for the National Infrastructure Coordination Center, or its successor, described in Strategic Imperative #1, which shall serve as the focal point for the protection and resilience of the physical aspects of the Nation's critical infrastructure. The functions shall include:
    a. In conjunction with the cyber coordination center, maintain a 24/7 situational awareness and crisis monitoring of critical infrastructure and share threat information, to reduce risk, prevent damage, and enable rapid recovery of critical infrastructure assets from incidents caused by natural disasters, attacks, or other emergencies;
    b. Work with appropriate SSAs and other Federal departments and agencies, SLTT entities, the private sector, academia, and international partners to protect and support mitigation and response efforts to incidents involving the physical aspects of the Nation's critical infrastructure;
    c. Compile and support analyses information about active threats and incidents that may impact the Nation's critical infrastructure;
    d. Facilitate information sharing, interaction, and collaboration among and between SSAs and other Federal department and agencies, critical infrastructure owners and operators, and international partners;

e. Maintain the ability to enable and support situational awareness and a common operating picture for critical infrastructure (that incorporates relevant cyber information) across private sector, Federal, SLTT, and international entities by integrating information obtained from such entities and providing relevant information to support the Secretary of Homeland Security in executing statutory responsibilities to provide the national common operating picture and to prevent attacks in the United States;
f. Disseminate timely and actionable threat, vulnerability, mitigation, and warning information to improve the security and protection of the Nation's critical infrastructure; and
g. Integrate Protective Security Advisors into the coordination centers.

4) Identify the responsibilities, location, and the array of cybersecurity functions for a Cyber coordination center, described in Strategic Imperative #1, which shall include:
   a. In conjunction with the physical infrastructure coordination center, maintain a 24/7 situational awareness and crisis monitoring capability for non-DoD Federal and private sector systems and cyber critical infrastructure, and disseminate timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information, including alerts, advisories, indicators, signatures, mitigation, and response measures;
   b. Coordination mechanisms for addressing shared responsibilities with other Federal departments and agencies; SLTT entities; the private sector; academia; and international partners to prevent and respond to cybersecurity threats and incidents involving non-DoD Federal and .com systems and other critical information infrastructure pursuant to the NCIRP, or its successor;
   c. With input from the Intelligence Community, an integration and analysis capability that compiles and analyzes information about known vulnerabilities and active threats and incidents that may impact non-DoD Federal and private sector systems and cyber infrastructure, including information voluntarily provided;
   d. An institutionalized capability to facilitate information sharing, interaction, and collaboration among and between agencies, SLTT entities, the private sector, academia, and international partners;
   e. Support efforts to integrate information from Federal government and non-Federal network operation centers and security operation centers to provide situational awareness and trend analysis regarding the Nation's information security posture and foster critical infrastructure information security collaboration among information system owners and operators;

f. Provide incident detection, analysis, mitigation, and response information, as well as remote or on-site technical assistance to heads of agencies and, upon request and if appropriate, governmental or private entities that own or operate cyber infrastructure;
g. Appropriately coordinate and integrate efforts with the National Infrastructure Coordination Center, or its successor; and
h. Carry out the responsibilities of the National Cybersecurity Center and the responsibilities of its director, and the functions and responsibilities of the Federal information security center required under the Federal Information Security Management Act (FISMA), which include the ability to enable and support situational awareness and a common operating picture for cyberspace across private sector, Federal, SLTT, and international entities by integrating information obtained from such entities and providing cyber information to support the Secretary of Homeland Security and his/her responsibilities to provide the national common operating picture and to prevent attacks in the United States.

5) The establishment of a physical infrastructure and cyber integration and analysis function that incorporates existing resources and DHS programs such as the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), National Infrastructure Simulation and Analysis Center (NISAC), expertise from the two integrated physical infrastructure and cyber coordination centers, and other relevant programs and capabilities to enable a comprehensive analysis function for critical infrastructure – both for steady state and incidents – at the intersection of the two critical infrastructure coordination centers. Its functions shall include:
    a. Conduct trend analysis to extract an underlying pattern or to predict future events;
    b. Pursue, in conjunction with the Intelligence Community, threat analysis to determine the seriousness of a threat and the likelihood it would be carried out; and
    c. Develop risk assessments at the intersection of threat and vulnerability to inform protective actions;
    d. Integrate physical infrastructure and cyber element information;
    e. Project potential impacts and cascading effects;
    f. Identify information requirements for the Intelligence Community to support analysis that enhances the protection and resilience of critical infrastructure; and
    g. Compile, assess, and integrate threat streams, hazard information and known vulnerabilities to aid in managing risks to critical infrastructure; project

interdependencies and cascading impacts; recommend protective measures; and support incident management and reconstitution of critical infrastructure.

2) Development of a National Plan, including an interim Outline and Schedule

The Secretary of Homeland Security, in coordination with the SSAs and other relevant Federal departments and agencies, and in collaboration with critical infrastructure owners and operators, independent and regulatory agencies, and SLTT entities, shall be responsible for developing a new national plan for critical infrastructure protection and resilience. The new national plan shall replace the current NIPP and convey overarching guidance to set a common compass heading, and identifying Executive Branch strategic functions and capabilities necessary to protect critical infrastructure.

Within 45 days of the date of this directive, the Secretary of Homeland Security shall provide to me, via the Assistant to the President for Homeland Security and Counterterrorism, an outline of the national plan and a schedule for the development of the plan not to exceed six months. The outline should include but is not limited to:

a. The updated Federal architecture and how it will support implementation of the plan;
b. A vision statement, goals, and strategic functions that reflect evolving threats and incorporate results from R&D and other advancements to protect critical infrastructure and enhance its resilience;
c. The method chosen to prioritize the Nation's critical infrastructure, define what it means, and explain how the strategic prioritization shall be used;
d. Identification of a risk management framework that it is adaptable, flexible, actionable, and measurable, and uses applicable R&D advancements to manage all hazards and the evolving threat environment;
e. A description of the protocols to be developed to synchronize communication and actions within the Federal Government – both in steady state and when there is a threat or incident that impacts National critical infrastructure, with appropriate linkages to the NCIRP, or its successor for cyber incidents;
f. The Energy and Communications Sectors shall be identified and incorporated into the mitigation and protection efforts across all sectors, and included in critical infrastructure strategic guidance and annual plans;
g. The metrics and analysis process that will be used to measure the Nation's ability to manage the risk and reduce that risk to critical infrastructure; and
h. Regular review to affirm alignment with PPD-8 deliverables and the NCIRP, or its successor, as appropriate.

3) Evolution of the Sector Coordination Structure

Numerous public-private coordination and information sharing structures exist for various purposes related to critical infrastructure. However, in an effort to increase the effectiveness of these mechanisms, to streamline processes and number of access points between public and private entities, and to minimize duplication of effort, the Federal government shall define a new focused, disciplined, and effective approach to coordinate with the critical infrastructure sectors and SLTT entities. This approach will include a U.S. government designated partner entity or entities and an articulation of the key functions to serve as a basis for an effective partnership. Within 60 days of the date of this directive, DHS will convene an Assistant Secretary-level meeting of the SSAs to develop and provide a recommendation to me, via the Assistant to the President for Homeland Security and Counterterrorism, which addresses:

a. Existing public-private coordination councils used to engage the critical infrastructure sectors for protection, resilience, and information sharing activities;
b. Other mechanisms or regular meetings/fora used to engage the critical infrastructure sectors for protection, resilience, and information sharing activities; and
c. Develop options for advancing an effective coordination framework that includes purpose, Federal access points, operational protocols, and implementation strategy, and also identifies other parts of the Federal government that interface with critical infrastructure owners and operators and how they will be made aware of these coordination mechanisms.

4) Development of an Information Exchange Framework

Within 120 days of the date of this directive, the Secretary of Homeland Security, in coordination with relevant Federal departments and agencies, shall provide an implementation plan to me, via the Assistant to the President for Homeland Security and Counterterrorism, to develop an information exchange framework for critical infrastructure between the Federal government and owners and operators of critical infrastructure and SLTT entities. The framework shall:

a. Leverage best practices from the National Counterterrorism Center, the National Infrastructure Advisory Council, and other information sharing entities;
b. Identify critical information business process requirements, including the type of information and thresholds (e.g., steady state, routine, local, national significance) for information to be exchanged;

c. Adopt standard operating procedures and standard methodologies for exchanging critical information, including for the automated exchange of indicators and warnings between operations centers in both the public and private sectors; and
d. Identify how and with whom information exchange will occur between Federal departments and agencies, and with owners and operators of critical infrastructure and SLTT entities.

5) Common Operating Picture for Critical Infrastructure

Within 180 days, the Secretary of Homeland Security shall demonstrate a near-real time common operating picture for critical infrastructure that includes threat streams and all hazards information along with vulnerabilities; provides the status of critical infrastructure and potential cascading effects; supports decision making; and disseminates critical information that may be needed to save or sustain lives, mitigate damage, and/or reduce further degradation of a critical infrastructure capability throughout an incident. This capability should be available for and cover physical and cyber elements of critical infrastructure, and enable an integration of information as necessitated by the incident.

6) Develop a Critical Infrastructure Protection and Resilience R&D Plan

Within two years of the date of this directive, the Secretary of Homeland Security, in coordination with the OSTP, the SSAs, DOC, and other Federal departments and agencies, shall provide to me, via the Assistant to the President for Homeland Security and Counterterrorism, a National Critical Infrastructure Protection and Resilience R&D 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 four years after its initial delivery, with interim updates as needed.

Policy coordination, dispute resolution, and periodic in-progress reviews for the implementation of this directive shall be carried out consistent with PPD-1, including the use of Interagency Policy Committee(s) under the leadership of the National Security Staff to develop policy documents.

Nothing in this directive alters, supersedes or impedes the ability of the heads of Federal departments and agencies, including independent or regulatory agencies, Federal committees, or the designated law enforcement and security services provider of a Federal department or agency, to carry out their authorities or to perform their responsibilities under law, consistent

with applicable legal authorities and other Presidential guidance, including but not limited to the designation of critical infrastructure under such authorities.

This directive supersedes and rescinds Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7), issued December 17, 2003. Plans developed under HSPD-7 shall remain in effect until they are superseded.

Designated Critical Infrastructure Sectors and Sector-Specific Agencies

This directive identifies the 16 critical infrastructure sectors and designates associated Federal SSAs. In some cases co-SSAs are designated where those departments share the roles and responsibilities of the SSA. The Secretary of Homeland Security shall periodically evaluate the need for and approve changes to critical infrastructure sectors in consultation with the Assistant to the President for Homeland Security and Counterterrorism. The sectors and SSAs are as follows:

Chemical:
Sector-Specific Agency: *Department of Homeland Security*

Commercial Facilities:
Sector-Specific Agency: *Department of Homeland Security*

Communications:
Sector-Specific Agency: *Department of Homeland Security*

Critical Manufacturing:
Sector-Specific Agency: *Department of Homeland Security*

Dams:
Sector-Specific Agency: *Department of Homeland Security*

Defense Industrial Base:
Sector-Specific Agency: *Department of Defense*

Emergency Services:
Sector-Specific Agency: *Department of Homeland Security*

Energy:
Sector-Specific Agency: *Department of Energy*

Financial Services:
Sector-Specific Agency: *Department of the Treasury*

Food and Agriculture:
Co-Sector-Specific Agencies: *U.S. Department of Agriculture and Department of Health and Human Services*

Government Facilities:
Co-Sector-Specific Agencies: *Department of Homeland Security and General Services Administration*

Healthcare and Public Health:
Sector-Specific Agency: *Department of Health and Human Services*

Information Technology:
Sector-Specific Agency: *Department of Homeland Security*

Nuclear Reactors, Materials, and Waste:
Sector-Specific Agency: *Department of Homeland Security*

Transportation Systems:
Co-Sector-Specific Agencies: *Department of Homeland Security and Department of Transportation*

Water and Wastewater Systems:
Sector-Specific Agency: *Environmental Protection Agency*

Definitions

For purposes of this directive:

The term "all hazards" describes a threat or an incident, natural or manmade, that warrants action to protect life, property, environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes, but is not limited to, natural disasters, cybersecurity incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure.

The term "collaboration" refers to the process of working together to achieve shared goals.

The terms "coordinate" and "in coordination with" denote a consensus decision-making process in which the named coordinating department or agency is responsible for working with the affected departments and agencies to achieve consensus and a consistent course of action.

The term "cyber critical infrastructure" includes information systems and other information infrastructure relied upon by critical infrastructure and Federal information systems (as defined in 40 U.S.C., Sec. 11331), but does not include DOD information systems.

The term "critical infrastructure" means 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, as defined in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)). This definition excludes national security systems.

The term "mission essential functions" are those functions that enable an organization to provide vital services, exercise civil authority, maintain safety and well-being of the general populace, and sustain industrial and economic base in an emergency.

The term "national security systems" has the meaning given to it in FISMA (44 U.S.C. § 3542(b)).

The term "protection" refers to those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. Protection also includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other physical or cybersecurity incidents, as well as a wide range of activities, such as hardening physical or virtual facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety, training and exercises, and implementing cybersecurity measures, among various others.

The term "resilience" refers to the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from steady state disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

The term "Sector-Specific Agency" (SSA), as defined by this policy, refers to the Federal department or agency responsible for leading, facilitating, and/or supporting the protection and resilience programs and activities of its designated critical infrastructure sector in the all hazards environment. SSAs will coordinate with DHS, other relevant Federal departments and

agencies, and collaborate with critical infrastructure owners and operators, independent and regulatory agencies, and SLTT entities to implement this directive.