DOWNLOAD PDF HOMELAND SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

Chapter 1 : Critical Infrastructure Protection - Homeland Security

The National Infrastructure Protection Plan (NIPP) provides a coordinated approach to critical infrastructure and key resource protection roles and responsibilities for federal, state, local, tribal, and private sector security partners.

Critical Infrastructure Security and Resilience The Presidential Policy Directive PPD on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. It includes distributed networks, varied organizational structures and operating models including multinational ownership , interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. 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. Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery. This directive establishes national policy on critical infrastructure security and resilience. This endeavor is a shared responsibility among the Federal, state, local, tribal, and territorial SLTT entities, and public and private owners and operators of critical infrastructure herein referred to as "critical infrastructure owners and operators". This directive also refines and clarifies the critical infrastructure-related functions, roles, and responsibilities across the Federal Government, as well as enhances overall coordination and collaboration. The Federal Government also has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators. Policy It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats. These efforts shall seek to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts related to critical infrastructure. The Federal Government shall also 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. This directive also identifies energy and communications systems as uniquely critical due to the enabling functions they provide across all critical infrastructure sectors. Three strategic imperatives shall drive the Federal approach to strengthen critical infrastructure security and resilience: All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions. Such infrastructure shall be addressed in the plans and execution of the requirements in the 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 privacy, civil rights, and civil liberties. In addition, Federal departments and agencies shall protect all information associated with carrying out this directive consistent with applicable legal authorities and policies. Roles and Responsibilities Effective implementation of this directive requires a national unity of effort pursuant to strategic guidance from the Secretary of Homeland Security. That national effort must include expertise and day-to-day engagement from the Sector-Specific Agencies SSAs as well as the specialized or support capabilities from other Federal departments and agencies, and strong collaboration with critical infrastructure owners and operators and SLTT entities. Additional roles and responsibilities for the Secretary of Homeland Security include: Sector-Specific Agencies Each critical infrastructure sector has unique characteristics, operating models, and risk profiles that benefit from an identified Sector-Specific Agency that has institutional knowledge and specialized expertise about the sector. Recognizing existing statutory or regulatory authorities of specific Federal departments and agencies, and leveraging existing sector familiarity and relationships, SSAs shall carry out the following roles and responsibilities for their respective

sectors: Additional Federal Responsibilities The following departments and agencies have specialized or support functions related to critical infrastructure security and resilience that shall be carried out by, or along with, other Federal departments and agencies and independent regulatory agencies, as appropriate. The Attorney General and the Secretary of Homeland Security shall collaborate to carry out their respective critical infrastructure missions. 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. Three Strategic Imperatives 1 Refine and Clarify Functional Relationships across the Federal Government to Advance the National Unity of Effort to Strengthen Critical Infrastructure Security and Resilience An effective national effort to strengthen critical infrastructure security and resilience must be guided by a national plan that identifies roles and responsibilities and is informed by the expertise, experience, capabilities, and responsibilities of the SSAs, other Federal departments and agencies with critical infrastructure roles, SLTT entities, and critical infrastructure owners and operators. During the past decade, new programs and initiatives have been established to address specific infrastructure issues, and priorities have shifted and expanded. As a result, Federal functions related to critical infrastructure security and resilience shall be clarified and refined to establish baseline capabilities that will reflect this evolution of knowledge, to define relevant Federal program functions, and to facilitate collaboration and information exchange between and among the Federal Government, critical infrastructure owners and operators, and SLTT entities. As part of this refined structure, there shall be two national critical infrastructure centers operated by DHS â€" one for physical infrastructure and another for cyber infrastructure. They shall function in an integrated manner and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect the physical and cyber aspects of critical infrastructure. Just as the physical and cyber elements of critical infrastructure are inextricably linked, so are the vulnerabilities. Accordingly, an integration and analysis function further developed in Strategic Imperative 3 shall be implemented between these two national centers. The success of these national centers, including the integration and analysis function, is dependent on the quality and timeliness of the information and intelligence they receive from the SSAs and other Federal departments and agencies, as well as from critical infrastructure owners and operators and SLTT entities. These national centers shall not impede the ability of the heads of Federal departments and agencies to carry out or perform their responsibilities for national defense, criminal, counterintelligence, counterterrorism, or investigative activities. This must facilitate the timely exchange of threat and vulnerability information as well as information that allows for the development of a situational awareness capability during incidents. The goal is to enable efficient information exchange through the identification of requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternate capabilities should there be a disruption in the primary systems. Greater information sharing within the government and with the private sector can and must be done while respecting privacy and civil liberties. Federal departments and agencies shall ensure that all existing privacy principles, policies, and procedures are implemented consistent with applicable law and policy and shall include senior agency officials for privacy in their efforts to govern and oversee information sharing properly. It shall reside at the intersection of the two national centers as identified in Strategic Imperative 1, and it shall include the capability to collate, assess, and integrate vulnerability and consequence information with threat streams and hazard information to: Aid in prioritizing assets and managing risks to critical infrastructure; b. Anticipate interdependencies and cascading impacts; c. Recommend security and resilience measures for critical infrastructure prior to, during, and after an event or incident; and d. Support incident management and restoration efforts related to critical infrastructure. This function shall not replicate the analysis function of the IC or the National Counterterrorism Center, nor shall it involve intelligence collection activities. This function shall also use information and intelligence provided by other critical infrastructure partners, including SLTT and nongovernmental analytic entities. Implementation of the Directive The

Secretary of Homeland Security shall take the following actions as part of the implementation of this directive. Within days of the date of this directive, the Secretary of Homeland Security shall develop a description of the functional relationships within DHS and across the Federal Government related to critical infrastructure security and resilience. It should include the roles and functions of the two national critical infrastructure centers and a discussion of the analysis and integration function. The Secretary shall coordinate this effort with the SSAs and other relevant Federal departments and agencies. The Secretary shall provide the description to the President through the Assistant to the President for Homeland Security and Counterterrorism. Within days of the date of this directive, the Secretary of Homeland Security, in coordination with the SSAs, other relevant Federal departments and agencies, SLTT entities, and critical infrastructure owners and operators, shall conduct an analysis of the existing public-private partnership model and recommend options for improving the effectiveness of the partnership in both the physical and cyber space. The evaluation shall consider options to streamline processes for collaboration and exchange of information and to minimize duplication of effort. Furthermore, the analysis shall consider how the model can be flexible and adaptable to meet the unique needs of individual sectors while providing a focused, disciplined, and effective approach for the Federal Government to coordinate with the critical infrastructure owners and operators and with SLTT governments. The evaluation shall result in recommendations to enhance partnerships to be approved for implementation through the processes established in the Organization of the National Security Council System directive. Within days of the date of this directive, the Secretary of Homeland Security, in coordination with the SSAs and other Federal departments and agencies, shall convene a team of experts to identify baseline data and systems requirements to enable the efficient exchange of information and intelligence relevant to strengthening the security and resilience of critical infrastructure. The experts should include representatives from those entities that routinely possess information important to critical infrastructure security and resilience; those that determine and manage information technology systems used to exchange information; and those responsible for the security of information being exchanged. Interoperability with critical infrastructure partners; identification of key data and the information requirements of key Federal, SLTT, and private sector entities; availability, accessibility, and formats of data; the ability to exchange various classifications of information; and the security of those systems to be used; and appropriate protections for individual privacy and civil liberties should be included in the analysis. The analysis should result in baseline requirements for sharing of data and interoperability of systems to enable the timely exchange of data and information to secure critical infrastructure and make it more resilient. The Secretary shall provide that analysis to the President through the Assistant to the President for Homeland Security and Counterterrorism. Within days of the date of this directive, the Secretary of Homeland Security shall demonstrate a near real-time situational awareness capability for critical infrastructure that includes threat streams and all-hazards information as well as 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, 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. Within days of the date of this directive, the Secretary of Homeland Security shall provide to the President, through the Assistant to the President for Homeland Security and Counterterrorism, a successor to the National Infrastructure Protection Plan to address the implementation of this directive, the requirements of Title II of the Homeland Security Act of as amended, and alignment with the National Preparedness Goal and System required by PPD The updated plan shall also reflect the identified functional relationships within DHS and across the Federal Government and the updates to the public-private partnership model. Finally, the plan should consider sector dependencies on energy and communications systems, and identify pre-event and mitigation measures or alternate capabilities during disruptions to those systems. The Secretary shall coordinate this effort with the SSAs, other relevant Federal departments and agencies, SLTT entities, and critical infrastructure owners and

operators. The plan should be issued every 4 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 Committees coordinated by the National Security Staff. Nothing in this directive alters, supersedes, or impedes the authorities of Federal departments and agencies, including independent regulatory agencies, to carry out their functions and duties consistent with applicable legal authorities and other Presidential guidance and directives, including, but not limited to, the designation of critical infrastructure under such authorities. Plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded. The Secretary of Homeland Security shall periodically evaluate the need for and approve changes to critical infrastructure sectors and shall consult with the Assistant to the President for Homeland Security and Counterterrorism before changing a critical infrastructure sector or a designated SSA for that sector. The sectors and SSAs are as follows: Department of Homeland Security Commercial Facilities: Department of Homeland Security Communications: Department of Homeland Security Critical Manufacturing: Department of Homeland Security Dams: Department of Defense Emergency Services: Department of Homeland Security Energy: Department of Energy Financial Services: Department of the Treasury Food and Agriculture: Department of Homeland Security Transportation Systems: Environmental Protection Agency Definitions For purposes of this directive: 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. The term "collaboration" means the process of working together to achieve shared goals. The terms "coordinate" and "in coordination with" mean 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 "Federal departments and agencies" means any authority of the United States that is an "agency" under 44 U. The term "national essential functions" means that subset of Government functions that are necessary to lead and sustain the Nation during a catastrophic emergency. The term "primary mission essential functions" means those Government functions that must be performed in order to support or implement the performance of the national essential functions before, during, and in the aftermath of an emergency. The term "national security systems" has the meaning given to it in the Federal Information Security Management Act of 44 U. The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. The term "Sector-Specific Agency" SSA means the Federal department or agency designated under this directive to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. The terms "secure" and "security" refer to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters.

Chapter 2 : House Committee on Homeland Security

The Office of Infrastructure Protection (IP) leads and coordinates national programs and policies on critical infrastructure security and resilience and has established strong partnerships across government and the private sector.

Chapter 3 : Critical Infrastructure

Critical infrastructure protection was the first subject on the list, Critical Infrastructure and Homeland Security Protection

Accomplishments." Jena Baker McNeill.

Chapter 4 : Homeland Security - Critical Infrastructure and Key Resources

Critical Infrastructure Protection The Office of Homeland Security is committed to enhancing the protection of Tennessee's critical infrastructure and key resources. Working cooperatively with federal, state and local government agencies, as well as the private sector, the Office of Homeland Security intends to build a safer, more secure.

Chapter 5 : Presidential Policy Directive -- Critical Infrastructure Security and Resilience | calendrierdelasci

The U.S. Department of Homeland Security provides strategic guidance and support to both public and private partners to promote a national unity of effort, and coordinate the overall goals to increase the security and resilience of America's critical infrastructure.

Chapter 6 : Critical Infrastructure Protection Plan (CIPP)

The Protected Critical Infrastructure Information (PCII) Program, managed by the U.S. Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD), is designed to encourage owners/operators of private sector critical infrastructure, key resources and significant special events (CIKR) to share sensitive, security.

Chapter 7 : Critical infrastructure protection - CHDS/Ed

Securing the nation's critical infrastructure has rightly become an increasingly vital component of a post-September 11 homeland security strategy.

Chapter 8 : DHS National Protection and Programs Directorate - Wikipedia

Cybersecurity and Infrastructure Protection Subcommittee. The Cybersecurity and Infrastructure Protection Subcommittee will legislate and oversee programs and issue areas of the U.S. Department of Homeland Security's (DHS) mission in cybersecurity and infrastructure protection.