

# Appendix 2: Authorities, Roles, and Responsibilities

## Appendix 2A: Summary of Relevant Statutes, Strategies, and Directives

This summary provides additional information on a variety of statutes, strategies, and directives referenced in chapters 2 and 5, as applicable to CI/KR protection. This list is not inclusive of all authorities related to CI/KR protection; rather, it includes the authorities most relevant to national-level, cross-sector CI/KR protection. Please note that there are many other authorities that are related to specific sectors that are not discussed in this appendix; these are left for further elaboration in the SSPs.

### 2A.1 Statutes

#### Homeland Security Act of 2002<sup>22</sup>

This act establishes a Cabinet-level department headed by a Secretary of Homeland Security with the mandate and legal authority to protect the American people from the continuing threat of terrorism. In the act, Congress assigns DHS the primary missions to:

- Prevent terrorist attacks within the United States;
- Reduce the vulnerability of the United States to terrorism at home;
- Minimize the damage and assist in the recovery from terrorist attacks that occur; and
- Ensure that the overall economic security of the United States is not diminished by efforts, activities, and programs aimed at securing the homeland.

This statutory authority defines the protection of CI/KR as one of the primary missions of the department. Among other actions, the act specifically requires DHS:

<sup>22</sup> Public Law 107-296, November 25, 2002, 116 Stat. 2135. It is codified at 6 U.S.C.

- To carry out comprehensive assessments of the vulnerabilities of the CI/KR of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks;
- To develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems; information technology and telecommunications systems (including satellites); electronic financial and property record storage and transmission systems; emergency preparedness communications systems; and the physical and technological assets that support such systems; and
- To recommend measures necessary to protect the CI/KR of the United States in coordination with other agencies of the Federal Government and in cooperation with State and local government agencies and authorities, the private sector, and other entities.

Those requirements, combined with the President’s direction in HSPD-7, mandate the unified approach to CI/KR protection taken in the NIPP.

### **Critical Infrastructure Information Act of 2002<sup>23</sup>**

Enacted as part of the Homeland Security Act, this act creates a framework that enables members of the private sector and others to voluntarily submit sensitive information regarding the Nation’s CI/KR to DHS with the assurance that the information, if it satisfies certain requirements, will be protected from public disclosure.

The PCII Program, created under the authority of the act, is central to the information-sharing and protection strategy of the NIPP. By protecting sensitive information submitted through the program, the private sector is assured that the information will remain secure and only be used to further CI/KR protection efforts.<sup>24</sup>

### **Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act)<sup>25</sup>**

The Stafford Act provides comprehensive authority for response to emergencies and major disasters—natural disasters, accidents, and intentionally perpetrated events. It provides specific authority for the Federal Government to provide assistance to State and local entities for disaster preparedness and mitigation, and major disaster and emergency assistance. Major disaster and emergency assistance includes such resources and services as:

- The provision of Federal resources, in general;
- Medicine, food, and other consumables;
- Work and services to save lives and restore property, including:
  - Debris removal;
  - Search and rescue; emergency medical care; emergency mass care; emergency shelter; and provision of food, water, medicine, and other essential needs, including movement of supplies or persons;
  - Clearance of roads and construction of temporary bridges;
  - Provision of temporary facilities for schools and other essential community services;
  - Demolition of unsafe structures that endanger the public;
  - Warning of further risks and hazards;
  - Dissemination of public information and assistance regarding health and safety measures;

<sup>23</sup> The CII Act is presented as subtitle B of title II of the Homeland Security Act (sections 211-215) and is codified at 6 U.S.C. 131 et seq.

<sup>24</sup> Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 8079 (Feb. 20, 2004), are codified at 6 CFR Part 29.

<sup>25</sup> Public Law 93-288, as amended, codified at 42 U.S.C. 68.

- Provision of technical advice to State and local governments on disaster management and control; and
- Reduction of immediate threats to life, property, and public health and safety;
- Hazard mitigation;
- Repair, replacement, and restoration of certain damaged facilities; and
- Emergency communications, emergency transportation, and fire management assistance.

### **Disaster Mitigation Act of 2000**

This act amends the Stafford Act by repealing the previous mitigation planning provisions (section 409) and replacing them with a new set of requirements (section 322). This new section emphasizes the need for State, Tribal, and local entities to closely coordinate mitigation planning and implementation efforts.

Section 322 continues the requirement for a State mitigation plan as a condition of disaster assistance, adding incentives for increased coordination and integration of mitigation activities at the State level through the establishment of requirements for two different levels of State plans—standard and enhanced. States that demonstrate an increased commitment to comprehensive mitigation planning and implementation through the development of an approved Enhanced State Plan can increase the amount of funding available through the Hazard Mitigation Grant Program (HMGP). Section 322 also established a new requirement for local mitigation plans and authorized up to 7 percent of HMGP funds available to a State to be used for development of State, local, and tribal mitigation plans.

### **Corporate and Criminal Fraud Accountability Act of 2002 (also known as the Sarbanes-Oxley Act)<sup>26</sup>**

The act applies to entities required to file periodic reports with the Securities and Exchange Commission under the provisions of the Securities and Exchange Act of 1934, as amended. It contains significant changes to the responsibilities of directors and officers, as well as the reporting and corporate governance obligations of affected companies. Among other things, the act requires certification by the company’s CEO and chief financial officer that accompanies each periodic report filed that the report fully complies with the requirements of the securities laws and that the information in the report fairly presents, in all material respects, the financial condition and results of the operations of the company. It also requires certifications regarding internal controls and material misstatements or omissions, and the disclosure on a “rapid and current basis” of information regarding material changes in the financial condition or operations of a public company. The act contains a number of additional provisions dealing with insider accountability and disclosure obligations, and auditor independence. It also provides severe criminal and civil penalties for violations of the act’s provisions.

### **The Defense Production Act of 1950 and the Defense Production Reauthorization Act of 2003**

This act provides the primary authority to ensure the timely availability of resources for national defense and civil emergency preparedness and response. Among other powers, this act authorizes the President to demand that companies accept and give priority to government contracts that the President “deems necessary or appropriate to promote the national defense,” and allocate materials, services, and facilities, as necessary, to promote the national defense in a major national emergency. This act also authorizes loan guarantees, direct loans, direct purchases, and purchase guarantees for those goods necessary for national defense. It also allows the President to void international mergers that would adversely affect national security. This act defines “national defense” to include critical infrastructure protection and restoration, as well as activities authorized by the emergency preparedness sections of the Stafford Act. Consequently, the authorities stemming from the Defense Production Act are available for activities and measures undertaken in preparation for, during, or following a natural disaster or accidental or malicious event. Under the act and related Presidential orders, the Secretary of Homeland Security has the authority to place and, upon application, authorize State and local governments to place priority-rated contracts in support of Federal, State, and local emergency preparedness activities. The Defense Production Act has a national security nexus with the NIPP. National emergencies related to CI/KR may arise that require the President to use his authority under the Defense Production Act.

<sup>26</sup> Public Law 107-204, July 30, 2002.

### **The Freedom of Information Act<sup>27</sup>**

This act generally provides that any person has a right, enforceable in court, to obtain access to Federal agency records, except to the extent that such records are protected from public disclosure by nine listed exemptions or under three law enforcement exclusions. Persons who make requests are not required to identify themselves or explain the purpose of the request. The underlying principle of FOIA is that the workings of government are for and by the people and that the benefits of government information should be made broadly available. All Federal Government agencies must adhere to the provisions of FOIA with certain exceptions for work in progress, enforcement confidential information, classified documents, and national security information. FOIA was amended by the Electronic Freedom of Information Act Amendment of 1996.

### **Information Technology Management Reform Act of 1996<sup>28</sup>**

Under section 5131 of the Information Technology Management Reform Act of 1996, NIST develops standards, guidelines, and associated methods and techniques for Federal computer systems. Federal Information Processing Standards are developed by NIST only when there are no existing voluntary standards to address the Federal requirements for the interoperability of different systems, the portability of data and software, and computer security.

### **Gramm-Leach-Bliley Act of 1999<sup>29</sup>**

Among other things, this act (title V) provides limited privacy protections on the disclosure by a financial institution of non-public personal information. The act also codifies protections against the practice of obtaining personal information through false pretenses.

### **Public Health Security and Bioterrorism Preparedness and Response Act of 2002<sup>30</sup>**

This act improves the ability of the United States to prevent, prepare for, and respond to bioterrorism and other public health emergencies. Key provisions of the act, 42 U.S.C. 247d and 300hh among others, address: (1) development of a national preparedness plan by HHS that is designed to provide effective assistance to State and local governments in the event of bioterrorism or other public health emergencies; (2) operation of the National Disaster Medical System to mobilize and address public health emergencies; (3) grant programs for the education and training of public health professionals and the improvement of State, local, and hospital preparedness for and response to bioterrorism and other public health emergencies; (4) streamlining and clarification of communicable disease quarantine provisions; (5) enhancement of controls on dangerous biological agents and toxins; and (6) protection of the safety and security of food and drug supplies.

### **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)<sup>31</sup>**

This act outlines the domestic policy related to deterring and punishing terrorists, and the U.S. policy for CI/KR protection. It also provides for the establishment of a national competence for CI/KR protection. The act establishes the NISAC and outlines the Federal Government's commitment to understanding and protecting the interdependencies among critical infrastructure.

### **The Privacy Act of 1974<sup>32</sup>**

This act provides strict limits on the maintenance and disclosure by any Federal agency of information on individuals that is maintained, including "education, financial transactions, medical history, and criminal or employment history and that contains [the] name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." Although there are specific categories for permissible maintenance of records and limited exceptions to the prohibition on disclosure for legitimate law enforcement and other specified purposes, the

<sup>27</sup> Codified as 5 U.S.C. 552.

<sup>28</sup> Public Law 104-106.

<sup>29</sup> Public Law 106-102 (1999), codified at 15 U.S.C. 94.

<sup>30</sup> Public Law 107-188.

<sup>31</sup> Public Law 107-56, October 26, 2001.

<sup>32</sup> Codified at 5 U.S.C. 552a.

act requires strict recordkeeping on any disclosure. The act also specifically provides for access by individuals to their own records and for requesting corrections thereto.

### **Federal Information Security Management Act of 2002<sup>33</sup>**

This act requires that Federal agencies develop a comprehensive information technology security program to ensure the effectiveness of information security controls over information resources that support Federal operations and assets. This legislation is relevant to the part of the NIPP that governs the protection of Federal assets and the implementation of cyber-protective measures under the Government Facilities SSP.

### **Cyber Security Research and Development Act of 2002<sup>34</sup>**

This act allocates funding to NIST and the National Science Foundation for the purpose of facilitating increased R&D for computer network security and supporting research fellowships and training. The act establishes a means of enhancing basic R&D related to improving the cyber security of CI/KR.

### **Maritime Transportation Security Act of 2002<sup>35</sup>**

This act directs initial and continuing assessments of maritime facilities and vessels that may be involved in a transportation security incident. It requires DHS to prepare a National Maritime Transportation Security Plan for deterring and responding to a transportation security incident and to prepare incident response plans for facilities and vessels that will ensure effective coordination with Federal, State, and local authorities. It also requires, among other actions, the establishment of transportation security and crewmember identification cards and processes; maritime safety and security teams; port security grants; and enhancements to maritime intelligence and matters dealing with foreign ports and international cooperation.

### **Intelligence Reform and Terrorism Prevention Act of 2004<sup>36</sup>**

This act provides sweeping changes to the U.S. Intelligence Community structure and processes, and creates new systems specially designed to combat terrorism. Among other actions, the act:

- Establishes a Director of National Intelligence with specific budget, oversight, and programmatic authority over the Intelligence Community;
- Establishes the National Intelligence Council and redefines “national intelligence”;
- Requires the establishment of a secure ISE and an information-sharing council;
- Establishes a National Counterterrorism Center, a National Counter Proliferation Center, National Intelligence Centers, and a Joint Intelligence Community Council;
- Establishes, within the Executive Office of the President, a Privacy and Civil Liberties Oversight Board;
- Requires the Director of the FBI to continue efforts to improve the intelligence capabilities of the FBI and to develop and maintain, within the FBI, a national intelligence workforce;
- Directs improvements in security clearances and clearance processes;
- Requires DHS to develop and implement a National Strategy for Transportation Security and transportation modal security plans; enhance identification and credentialing of transportation workers and law enforcement officers; conduct R&D into mass identification technology, including biometrics; enhance passenger screening and terrorist watch lists; improve measures for detecting weapons and explosives; improve security related to the air transportation of cargo; and implement other aviation security measures;

<sup>33</sup> Public Law 107-347, December 17, 2002.

<sup>34</sup> Public Law 107-305, November 27, 2002.

<sup>35</sup> Public Law 107-295, codified at 46 U.S.C. 701.

<sup>36</sup> Public Law 108-458.

- Directs enhancements to maritime security;
- Directs enhancements in border security and immigration matters;
- Enhances law enforcement authority and capabilities, and expands certain diplomatic, foreign aid, and military authorities and capabilities for combating terrorism;
- Requires expanded machine-readable visas with biometric data; implementation of a biometric entry and exit system, and a registered traveler program; and implementation of biometric or other secure passports;
- Requires standards for birth certificates and driver's licenses or personal identification cards issued by States for use by Federal agencies for identification purposes, and enhanced regulations for social security cards;
- Requires DHS to improve preparedness nationally, especially measures to enhance interoperable communications, and to report on vulnerability and risk assessments of the Nation's CI/KR; and
- Directs measures to improve assistance to and coordination with State, local, and private sector entities.

## 2A.2 National Strategies

### The National Strategy for Homeland Security (July 2002)

This strategy establishes the Nation's strategic homeland security objectives and outlines the six critical mission areas necessary to achieve those objectives. The strategy also provides a framework to align the resources of the Federal budget directly to the task of securing the homeland. The strategy specifies eight major initiatives to protect the Nation's CI/KR, one of which specifically calls for the development of the NIPP.

### National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003)

This strategy identifies the policy, goals, objectives, and principles for actions needed to "secure the infrastructures and assets vital to national security, governance, public health and safety, economy, and public confidence." The strategy provides a unifying organizational structure for CI/KR protection and identifies specific initiatives related to the NIPP to drive near-term national protection priorities and inform the resource allocation process.

### National Strategy to Secure Cyberspace (February 2003)

This strategy sets forth objectives and specific actions to prevent cyber attacks against America's CI/KR, reduce nationally identified vulnerabilities to cyber attacks, and minimize damage and recovery time from cyber attacks. The strategy provides the vision for cyber security and serves as the foundation for the cyber security component of CI/KR.

### The National Strategy for Maritime Security (September 2005)

This strategy provides the framework to integrate and synchronize the existing department-level strategies and ensure their effective and efficient implementation, and aligns all Federal Government maritime security programs and initiatives into a comprehensive and cohesive national effort involving appropriate Federal, State, local, and private sector entities.

### The National Strategy to Combat Weapons of Mass Destruction (December 2002)

This strategy provides policy guidance on combating WMD through three pillars:

- Counter proliferation to combat WMD use;
- Strengthened nonproliferation to combat WMD proliferation; and
- Consequence management to respond to WMD use.

### **The National Strategy for Combating Terrorism (February 2003)**

This strategy provides a comprehensive overview of the terrorist threat and sets specific goals and objectives to combat this threat, including measures to:

- Defeat terrorists and their organizations;
- Deny sponsorship, support, and sanctuary to terrorists;
- Diminish the underlying conditions that terrorists seek to exploit; and
- Defend U.S. citizens and interests at home and abroad.

### **The National Intelligence Strategy of the United States of America**

The National Intelligence Strategy of the United States of America outlines the fundamental values, priorities, and orientation of the Intelligence Community. As directed by the Director of National Intelligence, the strategy outlines the specific mission objectives that relate to efforts to predict, penetrate, and pre-empt threats to national security. To accomplish this, the efforts of the different enterprises of the Intelligence Community are integrated through policy, doctrine, and technology, and by ensuring that intelligence efforts are appropriately coordinated with the Nation's homeland security mission.

## **2A.3 Homeland Security Presidential Directives**

### **HSPD-1: Organization and Operation of the Homeland Security Council (October 2001)**

HSPD-1 establishes the Homeland Security Council and a committee structure for developing, coordinating, and vetting homeland security policy among executive departments and agencies. The directive provides a mandate for the Homeland Security Council to ensure the coordination of all homeland security-related activities among executive departments and agencies and promotes the effective development and implementation of all homeland security policies. The Homeland Security Council is responsible for arbitrating and coordinating any policy issues that may arise among the different departments and agencies under the NIPP.

### **HSPD-2: Combating Terrorism Through Immigration Policies (October 2001)**

HSPD-2 establishes policies and programs to enhance the Federal Government's capabilities for preventing aliens who engage in or support terrorist activities from entering the country, and for detaining, prosecuting, or deporting any such aliens who are in the United States.

HSPD-2 also directs the Attorney General to create the Foreign Terrorist Tracking Task Force to ensure that, to the maximum extent permitted by law, Federal agencies coordinate programs to accomplish the following: (1) deny entry into the United States of aliens associated with, suspected of being engaged in, or supporting terrorist activity; and (2) locate, detain, prosecute, or deport any such aliens already present in the United States.

### **HSPD-3: Homeland Security Advisory System (March 2002)**

HSPD-3 mandates the creation of an alert system for disseminating information regarding the risk of terrorist acts to Federal, State, and local authorities, and the public. It also includes the requirement for a corresponding set of protective measures for Federal, State, and local governments to be implemented, depending on the threat condition. Such a system provides warnings in the form of a set of graduated threat conditions that are elevated as the risk of the threat increases. For each threat condition, Federal departments and agencies are required to implement a corresponding set of protective measures.

### **HSPD-4: National Strategy to Combat Weapons of Mass Destruction (December 2002)**

This directive outlines a strategy that includes three principal pillars: (1) Counter-Proliferation to Combat WMD Use, (2) Strengthened Nonproliferation to Combat WMD Proliferation, and (3) Consequence Management to Respond to WMD

Use. It also outlines four cross-cutting functions to be pursued on a priority basis: (1) intelligence collection and analysis on WMD, delivery systems, and related technologies; (2) R&D to improve our ability to address evolving threats; (3) bilateral and multilateral cooperation; and (4) targeted strategies against hostile nations and terrorists.

#### **HSPD-5: Management of Domestic Incidents (February 2003)**

HSPD-5 establishes a national approach to domestic incident management that ensures effective coordination among all levels of government, and between the government and the private sector. Central to this approach is the NIMS, an organizational framework for all levels of government, and the NRP, an operational framework for national incident response.

In this directive, the President designates the Secretary of Homeland Security as the principal Federal official for domestic incident management and empowers the Secretary to coordinate Federal resources used for prevention, preparedness, response, and recovery related to terrorist attacks, major disasters, or other emergencies. The directive assigns specific responsibilities to the Attorney General, Secretary of Defense, Secretary of State, and the Assistants to the President for Homeland Security and National Security Affairs, and directs the heads of all Federal departments and agencies to provide their “full and prompt cooperation, resources, and support,” as appropriate and consistent with their own responsibilities for protecting national security, to the Secretary of Homeland Security, Attorney General, Secretary of Defense, and Secretary of State in the exercise of leadership responsibilities and missions assigned in HSPD-5.

#### **HSPD-6: Integration and Use of Screening Information (September 2003)**

HSPD-6 consolidates the Federal Government’s approach to terrorist screening by establishing a Terrorist Screening Center. Federal departments and agencies are directed to provide terrorist information to the Terrorist Threat Integration Center, which is then required to provide all relevant information and intelligence to the Terrorist Screening Center. In order to protect against terrorism, this directive established the national policy to: (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information, as appropriate and to the full extent permitted by law, to support (a) Federal, State, Territorial, local, tribal, foreign government, and private sector screening processes; and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.

#### **HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection (December 2003)**

HSPD-7 establishes a framework for Federal departments and agencies to identify, prioritize, and protect CI/KR from terrorist attacks, with an emphasis on protecting against catastrophic health effects and mass casualties. This directive establishes a national policy for Federal departments and agencies to identify and prioritize U.S. CI/KR and to protect them from terrorist attacks. HSPD-7 mandates the creation and implementation of the NIPP and sets forth roles and responsibilities for DHS; SSAs; other Federal departments and agencies; and State, local, tribal, private sector, and other security partners.

#### **HSPD-8: National Preparedness (December 2003)**

HSPD-8 establishes policies to strengthen the preparedness of the United States to prevent, protect, respond to, and recover from threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal; establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments; and outlining actions to strengthen the preparedness capabilities of Federal, State, and local entities. This directive mandates the development of the goal to guide emergency preparedness training, planning, equipment, and exercises, and to ensure that all entities involved adhere to the same standards. The directive calls for an inventory of Federal response capabilities and refines the process by which preparedness grants are administered, disbursed, and utilized at the State and local levels.

#### **HSPD-9: Defense of United States Agriculture and Food (January 2004)**

HSPD-9 establishes an integrated national policy for improving intelligence operations, emergency response capabilities, information-sharing mechanisms, mitigation strategies, and sector vulnerability assessments to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies.

### **HSPD-11: Comprehensive Terrorist-Related Screening Procedures (August 2004)**

HSPD-11 requires the creation of a strategy and implementation plan for a coordinated and comprehensive approach to terrorist screening in order to improve and expand procedures to screen people, cargo, conveyances, and other entities and objects that pose a threat.

### **HSPD-12: Policy for a Common Identification for Federal Employees and Contractors (August 2004)**

HSPD-12 establishes a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors in order to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy. The resulting mandatory standard was issued by NIST as the Federal Information Processing Standard Publication.

### **HSPD-13: Maritime Security Policy (December 2004)**

HSPD-13 directs the coordination of U.S. Government maritime security programs and initiatives to achieve a comprehensive and cohesive national effort involving the appropriate Federal, State, local, and private sector entities. The directive also establishes a Maritime Security Policy Coordinating Committee to coordinate interagency maritime security policy efforts.

### **HSPD-14: Domestic Nuclear Detection (April 2005)**

HSPD-14 establishes the effective integration of nuclear and radiological detection capabilities across Federal, State, local, and tribal governments and the private sector for a managed, coordinated response. This directive supports and enhances the effective sharing and use of appropriate information generated by the intelligence community, law enforcement agencies, counterterrorism community, other government agencies, and foreign governments, as well as providing appropriate information to these entities.

## **2A.4 Other Authorities**

### **Executive Order 13231, Critical Infrastructure Protection in the Information Age (October 2001) (amended by E.O. 13286, February 28, 2003)**

This Executive order provides specific policy direction to ensure protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. It recognizes the important role that networked information systems (critical information infrastructure) play in supporting all aspects of our civil society and economy and the increasing degree to which other critical infrastructure sectors have become dependent upon such systems. It formally establishes as U.S. policy the need to protect against disruption of the operation of these systems and to ensure that any disruptions that do occur are infrequent, of minimal duration, manageable, and cause the least damage possible. The Executive order specifically calls for the implementation of the policy to include “a voluntary public-private partnership, involving corporate and nongovernmental organizations.” The Executive order also reaffirms existing authorities and responsibilities assigned to various executive branch agencies and interagency committees to ensure the security and integrity of Federal information systems generally and of national security information systems in particular.

### **National Infrastructure Advisory Council**

In addition to the foregoing, Executive Order 13231 (as amended by E.O. 13286 of February 28, 2003, and E.O. 13385 of September 29, 2005) also established the NIAC as the President’s principal advisory panel on critical infrastructure protection issues spanning all sectors. The NIAC is composed of not more than 30 members, appointed by the President, who are selected from the private sector, academia, and State and local government, representing senior executive leadership expertise from the critical infrastructure and key resource areas as delineated in HSPD-7.

The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security of critical infrastructure, both physical and cyber, supporting important sectors of the economy. It also has the authority to provide advice directly

to the heads of other departments that have shared responsibility for critical infrastructure protection, including HHS, DOT, and DOE. The NIAC is charged to improve the cooperation and partnership between the public and private sectors in securing critical infrastructure and advises on policies and strategies that range from risk assessment and management, to information sharing, to protective strategies and clarification on roles and responsibilities between public and private sectors.

**Executive Order 12382, President's National Security Telecommunications Advisory Committee (amended by E.O. 13286, February 28, 2003)**

This Executive order creates the NSTAC, which provides to the President, through the Secretary of Homeland Security, information and advice from the perspective of the telecommunications industry with respect to the implementation of the National Security Telecommunications Policy.

**Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions (amended by E.O. 13286, February 28, 2003)**

Executive Order 12472 assigns NS/EP telecommunications functions, including wartime and non-wartime emergency functions, to the National Security Council, OSTP, Homeland Security Council, OMB, and other Federal agencies. The Executive order seeks to ensure that the Federal Government has telecommunications services that will function under all conditions, including emergency situations. This Executive order establishes the NCS with the mission to assist the President, the National Security Council, the Homeland Security Council, the Director of OSTP, and the Director of the OMB in: (1) the exercise of telecommunications functions and responsibilities set forth in the Executive Order; and (2) the coordination of planning for and provision of NS/EP communications for the Federal Government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution.