

# Appendix 1: Special Considerations

## Appendix 1A: Cross-Sector Cyber Security

This appendix provides additional details on the processes, procedures, and mechanisms needed to achieve NIPP goals and supporting objectives regarding cyber security. It specifies cyber security roles and responsibilities, coordination processes, initiatives to mitigate risk, and milestones and metrics to measure progress.

This appendix provides information concerning the users of cyber infrastructure, including the various CI/KR sectors and their associated security partners. Matters concerning *producers and providers* of cyber infrastructure (i.e., the Information Technology and Telecommunications sectors) are addressed in the SSPs. This appendix is organized to align with the corresponding chapters of the NIPP to provide the reader with the context for the additional information as follows:

- 1A.1 Introduction
- 1A.2 Responsibilities
- 1A.3 Managing Cyber Risk
- 1A.4 Ensuring Long-Term Cyber Security

### 1A.1 Introduction

The U.S. economy and national security are highly dependent upon cyber infrastructure. Cyber infrastructure enables the Nation's essential services, resulting in a highly interconnected and interdependent network of CI/KR. This network provides services supporting business processes and financial markets, and also assists in the control of many critical processes, including the electric power grid and chemical processing plants, among various others.

A spectrum of malicious actors can and do conduct attacks against critical cyber infrastructure on an ongoing basis. Of primary concern is the risk of organized cyber attacks capable of causing debilitating disruption to the Nation's CI/KR,

economy, or national security. Furthermore, while terrorist groups have not yet initiated a major attack against the Internet, there is evidence of their using it as a more limited means of attack or for other purposes that support terrorist activities.

DHS and the SSAs are committed to working collaboratively with other public, private, academic, and international entities to enhance cyber security awareness and preparedness efforts, and ensure that the cyber elements of CI/KR are:

- Robust enough to withstand attacks without incurring catastrophic damage;
- Responsive enough to recover from attacks in a timely manner; and
- Resilient enough to sustain nationally critical operations.

### 1A.1.1 Value Proposition for Cyber Security

The value proposition for cyber security aligns with that for CI/KR protection in general, as discussed in chapter 1 of the NIPP Base Plan, but with a concentrated focus on cyber infrastructure. Many CI/KR functions and services are enabled through cyber systems and services; if cyber security is not appropriately addressed, the risk to CI/KR is increased. The responsibility for cyber security spans all security partners, including public and private sector entities and individual citizens. The NIPP provides a coordinated and collaborative approach to help public and private sector security partners and individual citizens understand and manage cyber risk.

The NIPP promotes cyber security by facilitating participation and partnership in CI/KR protection initiatives, leveraging cyber-specific expertise and experience, and improving information exchange and awareness of cyber security concerns. It also provides a framework for public and private sector security partner efforts to recognize and address similarities and differences between approaches to cyber risk management for business continuity and national security. This framework enables security partners to work collaboratively to make informed cyber risk management decisions, define national cyber priorities, and address cyber security as part of an overall national CI/KR protection strategy.

### 1A.1.2 Definitions

The following definitions explain key terms and concepts related to the cyber dimension of CI/KR protection:

- **Cyber infrastructure:** Includes electronic information and communications systems and services and the information contained therein. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications includes sharing and distribution of information. For example, computer systems; control systems (e.g., SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure:
  - *Producers and providers* of cyber infrastructure represent the information technology industrial base, and comprise the Information Technology sector. The producers and providers of cyber infrastructure play a key role in developing secure and reliable products and services.
  - *Consumers* of cyber infrastructure must maintain its security as new vulnerabilities are identified and the threat environment evolves. Individuals, whether private citizens or employees with cyber systems administration responsibility, play a significant role in managing the security of computer systems to ensure that they are not used to enable attacks against CI/KR.
- **Cyber Security:** The prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems and services (and the information contained therein) to ensure confidentiality, integrity, and availability.

- **Cross-Sector Cyber Security:** Collaborative efforts between DHS, the SSAs, and other security partners to improve the cyber security of the CI/KR sectors by facilitating cyber risk-mitigation activities.

### **1A.1.3 Cyber-Specific Authorities**

Various Federal strategies, directives, policies, and regulations provide the basis for Federal actions and activities associated with implementing the cyber-specific aspects of the NIPP. The three primary authorities associated with cyber security are the National Strategy to Secure Cyberspace, HSPD-7, and the Homeland Security Act. These documents are described in further detail in appendix 2A of the NIPP.

## **1A.2 Cyber Security Responsibilities**

The National Strategy to Secure Cyberspace, HSPD-7, and the Homeland Security Act identify the responsibilities of the various security partners with a role in securing cyberspace. These roles and responsibilities are described in more detail below.

### **1A.2.1 Department of Homeland Security**

In accordance with HSPD-7, DHS is a principal focal point for the security of cyberspace. DHS has specific responsibilities regarding the coordination of the efforts of security partners to prevent damage to, unauthorized use and exploitation of, and enable the restoration of cyber infrastructure to ensure confidentiality, integrity, and availability. These responsibilities include:

- Developing a comprehensive national plan for securing U.S. CI/KR;
- Providing crisis management in response to incidents involving cyber infrastructure;
- Providing technical assistance to other government entities and the private sector with respect to emergency recovery plans for incidents involving cyber infrastructure;
- Coordinating with other Federal agencies to provide specific warning information and advice on appropriate protective measures and countermeasures to State, local, and tribal governments; the private sector; academia; and the public;
- Conducting and funding cyber security R&D, in partnership with other agencies, which will lead to new scientific understanding and technologies in support of homeland security; and
- Assisting SSAs in understanding and mitigating cyber risk and in developing effective and appropriate protective measures.

Within the risk management framework described in the NIPP, DHS is also responsible for the following activities:

- Providing cyber-specific expertise and assistance in addressing the cyber elements of CI/KR;
- Promoting a comprehensive national awareness program to empower businesses, the workforce, and individuals to secure their own segments of cyberspace;
- Working with security partners to reduce cyber vulnerabilities and minimize the severity of cyber attacks;
- Coordinating the development and conduct of national cyber threat assessments;
- Providing input on cyber-related issues for the National Intelligence Estimate of cyber threats to the United States;
- Facilitating cross-sector cyber analysis to understand and mitigate cyber risk;
- Providing guidance, review, and functional advice on the development of effective cyber-protective measures; and
- Coordinating cyber security programs and contingency plans, including recovery of Internet functions.

### 1A.2.2 Sector-Specific Agencies

Recognizing that each CI/KR sector possesses its own unique characteristics and operating models, SSAs provide the subject matter and industry expertise through relationships with the private sector to enable protection of the assets, systems, networks, and functions they provide within each of the sectors. SSAs must understand and mitigate cyber risk by:

- Identifying subject matter expertise regarding the cyber aspects of their sector;
- Increasing awareness of how the business and operational aspects of the sector rely on cyber systems and processes;
- Determining whether approaches for CI/KR inventory, risk assessment, and protective measures currently address cyber assets, systems, and networks; require enhancement; or require the use of alternative approaches;
- Reviewing and modifying existing and future sector efforts to ensure that cyber concerns are fully integrated into sector security strategies and protective activities;
- Establishing mutual assistance programs for cyber security emergencies; and
- Exchanging cyber-specific information with sector security partners, including the international community, as appropriate, to improve the Nation's overall cyber security posture.

### 1A.2.3 Other Federal Departments and Agencies

All Federal departments and agencies must manage the security of their cyber infrastructure while maintaining awareness of vulnerabilities and consequences to ensure that the cyber infrastructure is not used to enable attacks against the Nation's CI/KR. A number of Federal agencies have specific additional responsibilities outlined in the National Strategy to Secure Cyberspace:

- **The Department of Justice and the Federal Trade Commission:** Working with the sectors to address barriers to mutual assistance programs for cyber security emergencies.
- **The Department of Justice and Other Federal Agencies:**
  - Developing and implementing efforts to reduce or mitigate cyber threats by acquiring more robust data on victims of cyber crime and intrusions;
  - Leading the national effort to investigate and prosecute those who conduct or attempt to conduct cyber attacks;
  - Exploring means to provide sufficient investigative and forensic resources and training to facilitate expeditious investigation and resolution of CI/KR incidents; and
  - Identifying ways to improve cyber information sharing and investigative coordination among Federal, State, local, and tribal law enforcement communities; other agencies; and the private sector.
- **The Federal Bureau of Investigation and the Intelligence Community:** Ensuring a strong counterintelligence posture to deter intelligence collection against the Federal Government, as well as commercial and educational organizations.
- **The Intelligence Community, the Department of Defense, and Law Enforcement Agencies:** Improving the Nation's ability to quickly attribute the source of threats or attacks to enable timely and effective response.

### 1A.2.4 State, Local, and Tribal Governments

State, local, and tribal governments are encouraged to implement the following cyber recommendations:

- Managing the security of their cyber infrastructure while maintaining awareness of threats, vulnerabilities, and consequences to ensure that it is not used to enable attacks against CI/KR, and ensuring that government offices manage their computer systems accordingly;

- Participating in significant national, regional, and local awareness programs to encourage local governments and citizens to manage their cyber infrastructure appropriately; and
- Establishing cyber security programs, including policies, plans, procedures, recognized business practices, awareness, and audits.

### **1A.2.5 Private Sector**

The private sector is encouraged to implement the following recommendations as indicated in the National Strategy to Secure Cyberspace:

- Managing the security of their cyber infrastructure while maintaining awareness of vulnerabilities and consequences to ensure that it is not used to enable attacks against the Nation’s CI/KR;
- Participating in sector-wide programs to share information on cyber security;
- Evaluating the security of networks that affect the security of the Nation’s CI/KR, including:
  - Conducting audits to ensure effectiveness and the use of best practices;
  - Developing continuity plans that consider the full spectrum of necessary resources, including off-site staff and equipment; and
  - Participating in industry-wide information sharing and best practices dissemination;
- Reviewing and exercising continuity plans for cyber infrastructure and examining alternatives (e.g., diversity in service providers, implementation of recognized cyber security practices) as a way of improving resiliency and mitigating risk;
- Identifying near-term R&D priorities that include programs for highly secure and trustworthy hardware, software, and protocols; and
- Promoting more secure out-of-the-box installation and implementation of software industry products, including increasing user awareness of the security features of products; ease of use for security functions; and, where feasible, promotion of industry guidelines and best practices that support such efforts.

### **1A.2.6 Academia**

Colleges and universities are encouraged to implement several recommendations as indicated in the National Strategy to Secure Cyberspace:

- Managing the security of their cyber infrastructure while maintaining awareness of vulnerabilities and consequences to ensure that it is not used to enable attacks against the Nation’s CI/KR;
- Establishing appropriate information-sharing mechanisms to deal with cyber attacks and vulnerabilities;
- Establishing an on-call point of contact for Internet service providers and law enforcement officials in the event that the institution’s cyber assets, systems, or networks are discovered to be launching cyber attacks; and
- Establishing model guidelines empowering Chief Information Officers to manage cyber security, develop and exchange best practices for cyber security, and promote model user awareness programs.

### **1A.3 Managing Cyber Risk**

Under the NIPP, risk management follows a logical process that is comprised of the following fundamental activities:

(1) setting security goals; (2) identifying cyber assets, systems, networks, and functions; (3) assessing risk, which is based on consequences, threats, and vulnerability; (4) prioritizing efforts that maximize risk mitigation; (5) implementing protective programs; and (6) measuring effectiveness and improving programs. Each of these activities is discussed as they pertain to the cyber dimension of CI/KR protection in the subsections that follow.

#### **1A.3.1 Set Security Goals**

The goals and objectives set forth in the NIPP provide the overarching direction for CI/KR protection. Five cyber security objectives support the NIPP:

##### **Objective 1: Establish a National Cyberspace Security Response System**

Establishing a National Cyberspace Security Response System will improve the Nation's ability to prevent, protect against, detect, respond to, and reconstitute rapidly after a cyber incident by enhancing information exchange and analysis, improving situational awareness, and promoting collaboration and coordination among public, private, and international communities.

Section 1A.3.5 of this appendix describes various cyber security initiatives and programs, as well as exercise programs that promote effective collaborative response to cyber attack. Section 1A.4 of this appendix describes information sharing and international efforts to improve collaboration and coordination.

##### **Objective 2: Reduce Vulnerabilities and Minimize the Severity of Cyber Attacks**

Working with the public and private sectors to reduce vulnerabilities and minimize the severity of cyber attacks will help improve the security of CI/KR by reducing risks to cyber infrastructure, such as control systems.

Section 1A.3.5 of this appendix describes protective programs to reduce vulnerabilities and minimize the severity of cyber attacks.

##### **Objective 3: Raise National Awareness of Cyber Security**

Building and maintaining trusted relationships and enabling information exchange and collaboration with public, private, academic, and international partners will raise cyber security awareness. Raising national cyber security awareness, in turn, empowers businesses, the workforce, and individuals to secure their own segments of cyberspace.

Section 1A.4.1 of this appendix describes outreach and awareness initiatives to empower security partners at all levels of government and the private sector to secure cyberspace.

##### **Objective 4: Foster Cyber Training and Education**

Training and education are important components of establishing a knowledge base focused on the security of cyberspace. To foster adequate training and education to support the Nation's cyber security needs, a cadre of cyber security professionals must be developed and maintained through appropriate training and education programs.

Section 1A.4.3 of this appendix describes training and education programs designed to help develop cyber security professionals.

##### **Objective 5: Identify and Reduce Threats to Cyberspace**

Because of the ubiquitous nature of cyberspace, threats can emerge from anywhere at any time, and can be difficult to identify and track. Improving and coordinating cyber intelligence and threat detection and deterrence capabilities will help identify and reduce cyber threats.

Section 1A.4.1 of this appendix describes efforts to reduce cyber risk through improved interagency coordination.

### 1A.3.2 Identify Cyber Assets, Systems, Networks, and Functions

Cyber assets, systems, networks, and functions are examined as a key aspect of risk analysis. The process for identifying cyber assets, systems, networks, and functions should be repeatable, scalable, and distributable, and enable cyber interdependency analysis at both the sector and national levels to facilitate risk prioritization and mitigation.

Cyber assets, systems, and networks represent a variety of hardware and software components that perform a particular function. Examples of assets, systems, networks, and functions include networking equipment, database software, security systems, operating systems, local area networks, modeling and simulation, and electronic communications. The following are examples of cyber systems that exist in most, if not all, sectors and should be identified individually or included as a cyber element of a physical asset's description if the operation of that asset depends on them:

- **Business Systems:** Cyber systems used to manage or support common business processes and operations. Examples of business systems include Enterprise Resource Planning, e-commerce, e-mail, and R&D systems.
- **Control Systems:** Cyber systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. Control systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of control systems include SCADA, Process Control Systems, and Distributed Control Systems.
- **Access Control Systems:** Cyber systems allowing only authorized personnel and visitors physical access to defined areas of a facility. Access control systems provide monitoring and control of personnel passing throughout a facility by various means, including electronic card readers, biometrics, and radio frequency identification.

The Internet is a key resource comprised of domestic and international assets within both the Information Technology and Telecommunications sectors. It is used by all sectors to varying degrees. Availability of Internet service is the responsibility of both the Information Technology and Telecommunications sectors; however, the need for access to and reliance on the Internet are common to all sectors.

DHS, in collaboration with other security partners, provides a cross-sector cyber asset identification methodology that, when applied, enables a sector to identify cyber assets, systems, networks, and functions that may have nationally significant consequences if destroyed, incapacitated, or exploited. This methodology also characterizes the reliance of a sector's business and operational functionality on cyber assets, systems, and networks. Additional documentation on this methodology will be available in the near future. If an appropriate cyber asset identification methodology is already being used within the sector, DHS will work with the sector to ensure alignment of that methodology with the NIPP risk management framework described in chapter 3.

DHS also has ongoing efforts to ensure that the NADB and other CI/KR description databases used for risk assessment contain appropriate information on cyber assets, systems, networks, and functions.

### 1A.3.3 Assess Risks

Risk assessment for cyber assets, systems, and networks is an integral part of the risk management framework described in the NIPP. This framework combines consequences, threats, and vulnerabilities to produce systematic, comprehensive, and defensible risk assessments. DHS and the SSAs assess risk for cyber assets, systems, and networks associated with other CI/KR at the national and sector levels.

DHS and the SSAs will incorporate the results of these risk assessments into their overall risk management processes to prioritize where the Nation's limited resources for CI/KR protection activities should be applied.

**Consequence Analysis:** The first step in the risk assessment process involves determining the consequences of destruction; incapacitation; or exploitation of an asset, system, network, or the functions they provide.

To assess whether a given asset may be nationally consequential, physical, cyber, and human asset dependencies and interdependencies need to be assessed. Cyber interdependence presents a unique challenge for all sectors because of the borderless nature of cyberspace. Interdependencies are dual in nature (e.g., the Energy sector relies on computer-based control systems to manage the electric power grid, while those same control systems require electric power to operate).

Modeling and simulations through the NISAC will help quantify national and international dependency and interdependency, as well as their resulting consequences. However, this effort is highly complex and may not be appropriate for all assessments. When such advanced capability is not available or required, dependency and interdependency analyses may be carried out in a more subjective manner, with the participation of subject matter experts who have operational knowledge of the sectors involved, as well as the cross-sector interactions that are likely.

The consequences of cyber asset, system, or network destruction, incapacitation, or exploitation should be measured and described using a consistent system of measurements to ensure that the results can be compared across sectors. The NIPP provides baseline criteria for assessment methodologies to ensure such consistency. DHS also makes the RAMCAP process available for sectors to use at their discretion. While either of these approaches enables the consistent assessment of cyber consequences, both require that cyber assets, systems, networks, and functions be properly accounted for in the analysis process for the results to accurately reflect the consequences of cyber loss.

**Vulnerability Assessment:** The second step of the risk assessment process is analysis of vulnerability—determining which elements of infrastructure are most susceptible to attack and how attacks against these elements would most likely be carried out.

DHS works to identify cross-sector best practices to ensure that existing methodologies used by SSAs and other security partners address cyber vulnerabilities. DHS has taken a broad, inclusive approach by reviewing various existing, publicly available methods across government, industry, and academia to assemble a hybrid of the best practices. For example, DHS not only examines vulnerability standards from the International Organization for Standardization and NIST, but also studies vulnerability assessment methods used in the law enforcement and intelligence communities and the private sector.

DHS works to leverage established methodologies that have traditionally focused on physical vulnerabilities by enhancing them to better address cyber elements. Examples of these efforts include the enrichment of the Vulnerability Identification Self-Assessment Tool, as well as the RAMCAP process (see chapter 3).

There are cyber vulnerabilities that all sectors should consider when conducting their assessments, such as system interconnections. System interconnections (also known as trusted connections) are defined as the direct connection of two or more cyber systems owned by separate organizations. Business or government offices may interconnect for a variety of reasons, depending on the relationship between the interconnected entities. These interconnections may increase the security risk by exposing one system to vulnerabilities associated with another location.

**Threat Analysis:** The third step of the risk assessment process is the analysis of threat, which provides the likelihood that a target will be attacked. There are increasing indicators that potential adversaries intend to conduct cyber attacks and are actively acquiring cyber attack capabilities. Cyber attacks may not only target the Internet, but rather they may use it as a means of attack or for other purposes that support terrorist activities. Additionally, the increasing ease with which powerful cyber attack tools can be obtained and used puts the capability of conducting cyber attacks within reach of most groups or individuals who wish to do harm to the United States. However, credible information on specific adversaries is often not available. As such, DHS collaborates with the law enforcement and intelligence communities and the private sector to more accurately portray the possible ways in which the cyber threat may affect CI/KR, including the exploitation of the Internet as a weapon.

As called for in the National Strategy to Secure Cyberspace, DHS provides input on cyber-related issues for the National Intelligence Estimate of Cyber Threats to the U.S. Information Infrastructure. DHS will update its assessment on an annual basis to inform the general threat scenarios used in risk assessments and provide input to the National Intelligence Estimate as required.

The HITRAC conducts integrated threat analysis for CI/KR within DHS. HITRAC brings together intelligence and infrastructure specialists to ensure a complete and sophisticated understanding of the risks to U.S. CI/KR, including cyber infrastructure. To do this, HITRAC works in partnership with the U.S. Intelligence Community and national law enforcement to integrate and analyze intelligence and law enforcement information on the threat. It also works in partnership with the SSAs and owners and operators to ensure that their expertise on infrastructure operations is integrated into threat analysis. HITRAC combines intelligence, which includes all-source information, threat assessments, and trend analysis, with expert operational and practical knowledge, and an understanding of U.S. CI/KR to provide products for CI/KR risk assessment that include actionable conclusions regarding terrorist threats and risks. Additional information on HITRAC products can be found in section 3.3.4 of the NIPP Base Plan.

#### 1A.3.4 Prioritize

NIPP risk assessments provide comparable estimates of the risk faced by each CI/KR element and sector. This process allows key elements and sectors to be prioritized according to risk, and protective programs, including those focused on improving cyber security, to be designed that can help mitigate the highest priority risks. Those programs that offer the greatest risk mitigation for the dollars spent are afforded the highest priority. Although cyber-specific protective programs are frequently perceived to be costly, the costs of these programs may be significantly lower than the cascading costs associated with a successful cyber attack.

Cyber assets, systems, and networks and the functions they provide are prioritized using an overall risk-based approach. By integrating cyber threats, vulnerabilities, and consequences into risk analysis and by measuring risk in comparable terms for all elements and sectors, cyber assets, systems, networks, and functions are included in the prioritization process in a manner that ensures that they are appropriately considered along with other aspects of CI/KR.

#### 1A.3.5 Implement Protective Programs

Since each sector has a unique reliance on cyber infrastructure, DHS will assist the SSAs in developing a range of effective and appropriate cyber-protective measures.

In addition to individual sector-level protective measures, DHS has partnered with other public and private sector entities to develop and implement specific programs to help improve the security of the cyber infrastructure across sectors, as well as to support national cyber risk-mitigation activities, including:

- **Government Forum of Incident Response and Security Teams (GFIRST):** Following the model of the global FIRST organization, the Federal interagency community established the GFIRST to facilitate interagency information sharing and cooperation across Federal agencies for readiness and response efforts. GFIRST is a group of technical and tactical security response team practitioners responsible for securing government information technology systems. The members work together to understand and handle computer security incidents and to encourage proactive and preventive security practices.
- **Internet Disruption Working Group:** The Internet Disruption Working Group is a strategic partnership between public and private sector entities formed in response to concerns surrounding the dependency of critical communications, operations, and services on Internet functions. In addition to relying on the Internet for communications, many CI/KR sectors rely on the Internet to transfer operational information, conduct day-to-day business transactions, and perform essential services. The Internet Disruption Working Group is focused on identifying actions that government and other security partners can take in the near term to prepare for, protect against, and mitigate nationally significant Internet disruptions. In addressing the resiliency and recovery of Internet functions, the Internet Disruption Working Group is developing trusted relationships with the private sector, including key Internet infrastructure owners and operators.
- **The National Cyber Response Coordination Group:** The NCRCG member agencies use their established relationships with the private sector and State, local, and tribal governments to facilitate cyber incident management, develop courses of action, and devise appropriate response and recovery strategies. NCRCG facilitates coordination of the Federal

Government's efforts to prepare for, respond to, and recover from cyber incidents and physical attacks that have significant cyber consequences. Outlined in the NRP Cyber Annex, the NCRCG serves as the Federal Government's principal interagency mechanism for operational information sharing and coordination of Federal Government response and recovery efforts during a cyber crisis.

- **Programs for Federal Systems Cyber Security:** Federal prevention and protection efforts include those that are focused on securing cyber infrastructure owned and operated by the Federal Government. HSPD-7 mandates that “the heads of all Federal departments and agencies shall develop and submit to the Director of the OMB for approval plans for protecting the physical and cyber CI/KR that they own or operate. These plans address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities.” To assist Federal agencies in their efforts, DHS acts as a subject matter expert to OMB in reviewing the cyber aspects of Federal agency CI/KR plans to ensure that cyber risk is addressed consistently across all Federal agencies. DHS is working with the OMB to improve Federal civilian agency cyber security practices and compliance with the Federal Information Security Management Act.

In addition to the programs listed above, DHS operates the Cyber Exercise Program in coordination with the National Exercise Program. Through this program, DHS and security partners conduct exercises to improve coordination among members of the cyber incident response community. The program includes participation from Federal, State, local, tribal, and international government elements, as well as private sector corporations, coordinating councils, and academic institutions. The main objectives of national cyber exercises are to practice coordinated response to cyber attack scenarios; provide an environment for evaluation of interagency and cross-sector processes, procedures, and tools for communications and response to cyber incidents; and foster improved information sharing among government agencies and between government and private industry.

DHS, in collaboration with other security partners, has also established several vulnerability-reduction programs under the NIPP risk management framework, including:

- **Software Assurance Program:** Public and private sector security partners work together to develop best practices and new technologies to promote integrity, security, and reliability in software development. DHS leads the Software Assurance Program, a comprehensive effort that addresses people, processes, technology, and acquisition throughout the software life cycle. Focused on shifting away from the current security paradigm of patch management, these efforts will encourage the production of higher quality, more secure software. These efforts to promote a broader ability to routinely develop and deploy trustworthy software products through public-private partnerships are a significant element of securing cyberspace and the Nation's critical infrastructure. DHS also partners with NIST in the National Information Assurance Partnership (NIAP), a Federal Government initiative originated to meet the security testing needs of both information technology consumers and producers. NIAP is operated by NSA to address security testing, evaluation, and validation programs.
- **Control Systems Cyber Security Program:** The DHS Control Systems Cyber Security Program coordinates efforts among Federal, State, local, and tribal governments, as well as control system owners, operators, and vendors to improve control system security within and across all critical infrastructure sectors. The Control Systems Cyber Security Program coordinates activities to reduce the likelihood of success and severity of impact of a cyber attack against critical infrastructure control systems through risk-mitigation

**Control systems, which are critical components of our Nation's critical infrastructure, monitor and control sensitive processes and functions upon which our Nation depends (e.g., electricity generation, transmission, and distribution; natural gas production and distribution; transportation systems monitoring and control; water supply and treatment; and chemical processing).**

**Control systems historically were designed with proprietary solutions for specific uses in isolation, but are now frequently being implemented with remote access and open connectivity, utilizing common operating systems and, thus, are potentially vulnerable to various cyber attacks. Cyber security practices commonly implemented in business systems are often difficult to implement in operational control systems environments. As a result, cyber threats to control systems could potentially have devastating impacts on national security, economic security, public health and safety, as well as the environment.**

activities. These activities include assessing and managing control system vulnerabilities, assisting the US-CERT Control Systems Security Center with control system incident management, and providing control system situational awareness through outreach and training initiatives.

- **The Standards and Best Practices Program:** As part of its efforts to develop practical guidance and review tools, and promote R&D investment in cyber security, DHS and NIST co-sponsor the National Vulnerability Database. This database provides centralized and comprehensive vulnerability mitigation resources for all types of users, including the general public, system administrators, and vendors to assist with incident prevention and management (including links to patches) to mitigate consequences and vulnerabilities.

### 1A.3.6 Measure Effectiveness and Improve Programs

There are several core cyber measures and metrics that will be tracked within and across sectors to enable comparison and analysis between and among different types of critical infrastructure. DHS will work with security partners to develop descriptive, process, and outcome cyber core metrics to enable realistic evaluation of cyber security within and across sectors. The cyber core measures and metrics will parallel those being developed for the NIPP, and will also include the review, consideration, and integration of common cyber security policies, plans, procedures, and sound business practices, as appropriate. Separate sector-specific measures for cyber security may not be necessary in all cases; however, the sector-specific measures should strive to consider all sector assets, including cyber assets, systems, networks, and functions when measuring performance against goals.

Once the cyber core metrics have been developed and approved, DHS will establish a data-gathering and reporting process in cooperation with SSAs and other security partners to measure progress. This process will outline, but will not be limited to, the responsible parties, data collection and reporting methodology, and timeframes for data and metrics submissions. Additionally, as the process matures, additional metrics will be considered to reflect the most important issues currently being faced by the sectors.

The overall purpose of measuring effectiveness using metrics is to improve cyber CI/KR protection by mitigating risk. This means that using metrics as descriptors is not sufficient and that measured effectiveness must be compared to goals and improvements to enable the addressing of priority gaps.

## 1A.4 Ensuring Long-Term Cyber Security

The effort to ensure a coherent cyber CI/KR protection program over the long term has four components that are described in greater detail below:

- **Information Sharing and Awareness:** Ensures implementation of effective, coordinated, and integrated protection of cyber assets, systems, and networks, and the functions they provide, and enables cyber security partners to make informed decisions with regard to short- and long-term cyber security postures, risk mitigation, and operational continuity.
- **International Cooperation:** Promotes a global culture of cyber security and improves overall cyber incident preparedness and response posture.
- **Training and Education:** Ensures that skilled and knowledgeable cyber security professionals are available to undertake NIPP programs in the future.
- **Research and Development:** Improves cyber security protective capabilities or dramatically lowers the costs of existing capabilities so that State, local, tribal, and private sector security partners can afford to do more with their limited budgets.

### 1A.4.1 Information Sharing and Awareness

Information sharing and awareness involves sharing programs with agency partners and other security partners, and special sharing arrangements for emergency situations. Each of these is discussed below:

**Interagency Coordination:** Interagency cooperation and information sharing are essential to improving national cyber counterintelligence and law enforcement capabilities. The intelligence and law enforcement communities have both official and informal mechanisms in place for information sharing that DHS supports:

- **FBI's Cyber Task Forces** involve more than 50 law enforcement agency cyber task forces and more than 80 additional cyber working groups throughout the country, collaborating with Federal, State, and local partners to maximize investigative resources to ensure a timely and effective response to cyber security threats of both a criminal and national security nature.
- **Cybercop Portal** is a secure Internet-based information-sharing mechanism for more than 5,300 law enforcement members involved in the field of electronic crimes investigations. The law enforcement community, including investigators from private industry (e.g., banks and the network security community), is tied together and supported by this secure, Internet-based collaboration portal.
- **FBI's InfraGard** program is a public-private partnership coordinated out of the 56 FBI field offices nationwide. The program brings together law enforcement, academia, and private sector entities on a monthly basis to provide a forum for information sharing and networking.
- **FBI's Inter-Agency Coordination Cell** is a multi-agency group focused on sharing law enforcement information on cyber-related investigations.
- **U.S. Secret Service's Electronic Crimes Task Forces** provide interagency coordination on cyber-based attacks and intrusions.

**Information Sharing and Analysis Centers:** Underscoring effective cyber security efforts is the importance of information sharing between and among industry and government. To this end, the Information Technology and Communications ISACs work closely together and with DHS and the SSAs to maximize resources, coordinate preparedness and response efforts, and maintain situational awareness to enable risk mitigation regarding cyber infrastructure.

**Cyber Security Awareness for Security Partners:** DHS plays an important leadership role in coordinating a public-private partnership to promote and raise cyber security awareness among the general public by:

- Partnering with other Federal and private sector organizations to sponsor the National Cyber Security Alliance (NCSA), including creating a public-private organization, Stay Safe Online, to educate home users, small businesses, and K-12 and higher education audiences on cyber security best practices.
- Engaging with the MS-ISAC to help enhance the Nation's cyber security readiness and response at the State and local levels, and launching a national cyber security awareness effort in partnership with the MS-ISAC. The MS-ISAC is an information-sharing organization, with representatives of State and local governments, that analyzes, sanitizes, and disseminates information pertaining to cyber events and vulnerabilities to its constituents and private industry.
- Collaborating with the NCSA, the MS-ISAC, and the public and private sector to establish October as National Cyber Security Awareness Month and participating in activities to continuously raise cyber security awareness nationwide.

**Cyberspace Emergency Readiness:** DHS established the US-CERT, which is a 24/7 single point of contact for cyberspace analysis and warning, information sharing, and incident response and recovery for a broad range of users, including government, enterprises, small businesses, and home users. US-CERT is a partnership between DHS and the public and private sectors designed to help secure the Nation's Internet infrastructure and to coordinate defenses against and responses to cyber attacks across the Nation. US-CERT is responsible for:

- Analyzing and reducing cyber threats and vulnerabilities;
- Disseminating cyber threat warning information; and
- Coordinating cyber incident response activities.

To support the information-sharing requirements of the network approach, US-CERT provides the following information on their Web site, accessible via the HSIN, and via mailing lists:

- **Cyber Security Alerts:** Written in a language for home, corporate, and new users, these alerts are published in conjunction with technical alerts in the context of security issues that affect the general public.
- **Cyber Security Bulletins:** Bulletins summarize information that has been published regarding emergent security issues and vulnerabilities. They are published weekly and are written primarily for systems administrators and other technical users.
- **Cyber Security Tips:** Tips provide information and advice on a variety of common cyber security topics. They are published biweekly and are written primarily for home, corporate, and new users.
- **National Web Cast Initiative:** In an effort to increase cyber security awareness and education among the States, DHS, through US-CERT, and the MS-ISAC have launched a joint partnership to develop a series of national Web casts that will examine critical and timely cyber security issues. The purpose of the initiative is to strengthen the Nation's cyber readiness and resilience.
- **Technical Cyber Security Alerts:** Written for systems administrators and experienced users, technical alerts provide timely information on current cyber security issues, vulnerabilities, and exploits.

US-CERT also provides a method for citizens, businesses, and other institutions to communicate and coordinate directly with the Federal Government on matters of cyber security. The private sector can use the protections afforded by the Protected Critical Infrastructure Information Act to electronically submit proprietary data to US-CERT.

#### 1A.4.2 International Coordination on Cyber Security

The Federal Government proactively uses its intelligence capabilities to protect the country from cyber attack, its diplomatic outreach and operational capabilities to build partnerships in the global community, and its law enforcement capabilities to combat cyber crime wherever it originates. The private sector, international industry associations, and companies with global interests and operations are also engaged in addressing cyber security internationally. For example, the U.S.-based Information Technology Association of America participates in international cyber security conferences and forums, such as the India-based National Association for Software and Service Companies Joint Conference. These efforts involve interaction with both the policy and operational communities to coordinate national and international activities that are mutually supportive across the globe:

- **International Cyber Security Outreach:** DHS, in conjunction with the Department of State and other Federal agencies, engages in multilateral and bilateral discussions to further international security awareness and policy development, as well as incident response team information-sharing and capacity-building objectives. The United States engages in bilateral discussions on important cyber security issues with close allies and others with whom the United States shares networked interdependencies, to include, but not limited to: Australia, Canada, Egypt, Germany, Hungary, India, Italy, Japan, the Netherlands, Romania, the United Kingdom, etc. The United States also provides leadership in multilateral and regional forums addressing cyber security and CI/KR protection to encourage all nations to take systematic steps to secure their networked systems. For example, U.S. initiatives include: the Asia-Pacific Economic Cooperation Telecommunications Working Group capacity-building program to help member countries develop CSIRTs, and the OAS framework proposal to create a regional computer incident response points-of-contact network for information sharing and to help member countries develop CSIRTs. Other U.S. efforts to build a culture of cyber security include participation in OECD, G8, and

United Nations activities. The U.S. private sector is actively involved in this international outreach in partnership with the Federal Government.

- **Collaboration on Cyber Crime:** The U.S. outreach strategy for comprehensive cyber laws and procedures draws on the Council of Europe Convention on Cyber Crime, as well as: (1) the G8 High-Tech Crime Working Group's principles for fighting cyber crime and protecting critical information infrastructure, (2) the OECD guidelines on information and network security, and (3) the United Nations General Assembly resolutions based on the G8 and OECD efforts. The goal of this outreach strategy is to encourage individual nations and regional groupings of nations to join DHS in efforts to protect internationally interconnected national systems.
- **Collaborative Efforts for Cyber Watch, Warning, and Incident Response:** The Federal Government is working strategically with key allies on cyber security policy and operational cooperation. For example, DHS is leveraging pre-existing relationships among CSIRTs. DHS also has established a preliminary framework for cooperation on cyber security policy, watch, warning, and incident response with key allies. The framework also incorporates efforts related to key strategic issues as agreed upon by these allies. An IWWN is being established among cyber security policy, computer emergency response, and law enforcement participants representing 15 countries. The IWWN will provide a mechanism for the participating countries to share information to build global cyber situational awareness and coordinate incident response.
- **Partnerships to Address Cyber Aspects of Critical Infrastructure Protection:** DHS and the SSAs are leveraging existing agreements, such as the SPP and the JCG with the United Kingdom, to address the Information Technology sector and cross-cutting cyber components of CI/KR protection. The trilateral SPP builds on existing bilateral agreements between the United States and Canada and the United States and Mexico by allowing issues to be addressed on a dual bi-national basis. In the context of the JCG, DHS established a 10-point action plan to address cyber security, watch, warning, and incident response and other strategic initiatives.

### 1A.4.3 Training and Education

The National Strategy to Secure Cyberspace highlights the importance of cyberspace security training and education. Education and training are strategic initiatives in which DHS and other Federal agencies are actively engaged to affect a greater awareness and participation in efforts to promote cyber security for the future.

The Federal Government has undertaken several initiatives in partnership with the research and academic communities to better educate and train future cyber security practitioners:

- DHS co-sponsors the National CAEIAE program with NSA. Together, DHS and NSA are working to expand the program nationally.
- DHS collaborates with the National Science Foundation to co-sponsor and expand the Cyber Corps Scholarship for Service program. The Scholarship for Service program provides grant money to selected CAEIAE and other universities with programs of a similar caliber to fund the final 2 years of bachelor's, master's, or doctoral study in information assurance in exchange for an equal amount of time spent working for the Federal Government.
- In fiscal year 2004, the joint DHS/Treasury Computer Investigative Specialist program trained 48 Federal criminal investigators in basic computer forensics. Agents from ICE, the Internal Revenue Service, and the U.S. Secret Service attended the basic 6½-week course. This training was funded through the Treasury Executive Office of Asset Forfeiture.
- DHS is collaborating with DOD to finalize a comprehensive information technology job skills standard to guide development of a national certification program for security professionals within the Federal Government and private industry.
- Through DHS, DOJ, DOD, and the Department of State, the Federal Government provides cyber-related training to foreign cyber incident responders (incident response management, creation of CSIRTs) and law enforcement personnel and jurists (laws, computer forensics, case handling).

#### **1A.4.4 Research and Development**

The Cyber Security Research and Development Act of 2002 authorized a multi-year effort to create more secure cyber technologies, expand cyber security R&D, and improve the cyber security workforce.

To further address cyber R&D needs, the White House's OSTP established a CSIA IWG under the NSTC. The CSIA IWG was jointly chartered by NSTC's Subcommittee on Networking and Information Technology R&D and the Subcommittee on Infrastructure. This interagency working group includes participation from 20 organizations representing 11 departments and agencies, as well as from several offices in the White House.

The purpose of the working group is to coordinate Federal programs for cyber security and information assurance R&D. It also is responsible for developing the Federal Plan for Cyber Security and Information Assurance R&D, which includes near-term, mid-term, and long-term cyber security research efforts in response to the National Strategy to Secure Cyberspace and HSPD-7. The document includes descriptions of approximately 50 cyber security R&D topics, such as Automated Attack Detection, Warning, and Response; Forensics, Traceback, and Attribution; Security Technology and Policy Management Methods; Policy Specification Languages; and Integrated, Enterprise-Wide Security Monitoring and Management. The document also identifies the top cyber security and information assurance research topics across the Federal Government. Finally, the document includes key findings and recommendations. DHS actively co-chairs the CSIA IWG with OSTP and continues to identify critical cyber R&D requirements for incorporation into Federal R&D planning efforts.

#### **1A.4.5 Exploring Private Sector Incentives**

Awareness and understanding of the need for cyber security present a challenge for both government and industry. Although cyber security requires significant investments in time and resources, an effective cyber security program may reduce the likelihood of a successful cyber attack or the impact if a cyber attack occurs. Network disruptions resulting from cyber attacks can lead to loss of money, time, products, reputation, sensitive information, or even potential loss of life through cascading effects on critical systems and infrastructure. From an economic perspective, cyber attacks have resulted in billions of dollars of business losses and damages in the aggregate.

The private sector makes risk management decisions, including those for cyber security, based on return on investment and ensuring business continuity. Market-based incentives for cyber security investments include protection of intellectual capital, security-influenced procurement, market differentiation, and public confidence. Sometimes, however, cyber assets, systems, networks, or functions may be deemed nationally critical and necessitate additional risk management beyond that which the private sector implements as part of their corporate responsibility. To address this difference, DHS is collaborating with the public and private sectors through various programs and outreach efforts (e.g., US-CERT, the Control Systems Cyber Security Program, and the Software Assurance Program) to promote awareness of cyber security risks, and create incentives for increased investment in cyber security.

