

6. Ensuring an Effective, Efficient Program Over the Long Term

This chapter addresses the efforts needed to ensure an effective, efficient CI/KR protection program over the long term. It focuses particularly on the long-lead-time elements of CI/KR protection that require sustained plans and investments over time, such as generating skilled human capital, developing high-tech systems, and building public awareness.

Key activities needed to enhance CI/KR protection over the long term include:

- **Building national awareness** to support the CI/KR protection program, related protection investments, and protection activities by ensuring a focused understanding of the all-hazards threat environment and of what is being done to protect and enable the timely restoration of the Nation's CI/KR in light of such threats;
- **Enabling education, training, and exercise programs** to ensure that skilled and knowledgeable professionals and experienced organizations are able to undertake NIPP-related responsibilities in the future;
- **Conducting R&D and using technology** to improve protective capabilities or to lower the costs of existing capabilities so that security partners can afford to do more with limited budgets;
- **Developing, protecting, and maintaining data systems and simulations** to enable continuously refined risk assessment within and across sectors and to ensure preparedness for domestic incident management; and

- **Continuously improving the NIPP** and associated plans and programs through ongoing management and revision, as required.

6.1 Building National Awareness

The development and implementation of a national awareness program for CI/KR protection was identified as a major need in the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets. DHS, in conjunction with the SSAs and other security partners, is responsible for developing and implementing a comprehensive national awareness program that supports the sustainability of CI/KR protection, security investments, and focused public and private sector understanding of the CI/KR all-hazards risk environment.

The objectives of the national awareness program are to:

- Incorporate CI/KR protection and restoration considerations into business planning and operations, including employee and senior manager education and training programs, across all levels of government and the private sector;

- Support public and private sector decisionmaking and enable the planning of relevant and effective protection and restoration strategies and inform resource allocation processes;
- Develop an understanding of CI/KR dependencies and interdependencies and the value of cross-sector CI/KR protection and restoration planning down to the community level;
- Maintain public understanding of the evolving threat to CI/KR as assessed by the intelligence community and in the context of the HSAS; and
- Build public understanding of efforts to address the threat environment and enhance protection and rapid restoration of the Nation's CI/KR.

DHS and other Federal agencies are also engaged in a comprehensive national cyberspace security awareness campaign to remove impediments to sharing vulnerability information among security partners. This campaign includes audience-specific awareness materials, expansion of the Stay Safe Online campaign, and development of awards programs for those in industry who make significant contributions to the effort.

6.2 Enabling Education, Training, and Exercise Programs

The NIPP establishes a framework to enable the education, training, and exercise programs that allow people and organizations to develop and maintain key CI/KR protection expertise. Building the requisite individual and organizational expertise requires attracting, training, and maintaining sufficient numbers of professionals who have the particular expertise unique or essential to CI/KR protection. This, in turn, requires individual education and training to develop and maintain the requisite levels of expertise through technical, academic, and professional development programs. It also requires organizational training and exercises to develop the requisite organizational-level expertise. The framework that the NIPP establishes to enable each of these is discussed below.

6.2.1 Types of Expertise for CI/KR Protection

Some types of CI/KR protection expertise are associated with well-established disciplines that already feature formal academic education programs, recognized technical training levels and credentials, and professional certification systems

implemented through professional organizations or government licensing. Others involve unique skills and professional expertise that are specific to CI/KR protection, such as the expertise needed to implement the NIPP risk management framework. Such expertise often involves cutting-edge approaches that are not yet widely practiced and have yet to develop academic degrees or professional certification mechanisms in a nationwide system. The NIPP focuses special emphasis on the types of expertise that are unique to or essential for CI/KR protection. These include:

- Risk assessment and risk management and related concepts used in business continuity planning;
- Cost-benefit analysis to inform risk management priorities;
- Resource allocation based on risk management priorities;
- Analysis of insider threats to CI/KR and applicable countermeasures;
- Analysis of physical and cyber threats to CI/KR, including control systems, and cyber security measures;
- CI/KR dependency and interdependency analyses;
- International aspects of CI/KR protection;
- Best practices and technical capabilities for CI/KR protection, business continuity, and resiliency; and
- Best practices and technical capabilities for information sharing and protection.

6.2.2 Individual Education and Training

The NIPP recognizes the importance of leveraging existing accredited academic programs, professional certification standards, and technical training programs that are in place for the more mature and established disciplines. Whether CI/KR protection disciplines are established or newly evolving, they must include the technical, academic, and professional skill sets upon which the NIPP and SSPs are based. This requires an effort with a national scope that includes, but is not limited to, the following components:

- Technical training to provide individuals with the skills needed to perform their roles and responsibilities under the NIPP;
- Academic and research programs that result in formal degrees from accredited institutions; and
- Professional continuing education, which incorporates the latest advances in CI/KR risk-mitigation approaches and,

where appropriate, certification based on government, industry, and professional organization standards.

To enable each of these components, the NIPP specifies areas of emphasis that are discussed in the subsections that follow.

6.2.2.1 Technical CI/KR Protection Training

Training that is technical in nature can be grouped into two major categories: (1) specific technical training on the details of the NIPP itself for staff and decisionmakers, and (2) broader operational training for those charged with implementing CI/KR protection programs or who work in a CI/KR facility or operate a critical system or network. Each are described below:

- **Specialized NIPP Training:** Training for managers and staff responsible for NIPP implementation should provide an awareness level of training on all aspects of the NIPP, including, but not limited to, the underlying authorities; responsibilities; risk management framework; sector partnership model; information sharing; protection program requirements; and planning, resource, and budget processes. The basic awareness-level training should also provide participants with a working knowledge of how to use the NIPP and apply its principles and processes, both for steady-state CI/KR protection and to enable the CI/KR protection dimension of domestic incident management.

DHS will provide or coordinate the development of course materials on these topics; work with security partners, SCCs, and GCCs to facilitate the definition of general training requirements; and guide the development of national-level training standards associated with the NIPP. DHS will facilitate initial training in these topics for security partners, as appropriate.

- **Operational CI/KR Protection Training:** Technical CI/KR protection training programs for security partners enhance the knowledge and skills required to detect, deter, defend, and mitigate against terrorist activities and other incidents and events that threaten CI/KR. DHS and other Federal agencies support and provide training resources to local law enforcement officers and others, with a special focus on urban areas with significant clusters of CI/KR, localities where high-profile special events are typically scheduled, or other potentially high-risk geographical areas or jurisdictions. Federally provided technical training courses cover a range of operational and technical topics, such as buffer zone protection, bombing prevention, workforce terrorism awareness, surveillance detection, high-risk target awareness, and WMD incident training.

DHS also supports cyber security training, education, and awareness programs by educating vendors and manufacturers on the value of pre-configuring security options in products so that they are secure on initial installation; educating users on secure installation and use of cyber products; increasing user awareness and ease of use of the security features in products; and, where feasible, promotion of industry guides. These training efforts also encourage programs that leverage the existing Cyber Corps Scholarship for Service program, as well as various graduate and post-doctoral programs; link Federal cyber security and computer forensics training programs; and establish cyber security programs for departments and agencies, including awareness, audits, and standards as required.

Other Federal agencies also offer training related to CI/KR protection. For example, the Office of Personnel Management and DOD offer courses on CI/KR target awareness and best practices risk-mitigation measures. The Department of the Treasury also works with DHS to jointly provide training for criminal investigators in basic computer forensics.

DHS solicits recommendations from national professional organizations and from Federal, State, local, tribal, and private sector security partners for additional discipline-specific technical training courses related to CI/KR protection, and supports course development as appropriate.

6.2.2.2 Academic and Research Programs

DHS works with a wide range of academic institutions to incorporate CI/KR protection into professional education programs. For example, DHS collaborates with universities to incorporate a security-related curriculum into business school programs under Project MBA (master's of business administration) to better prepare the Nation's future business leaders to plan, implement, and manage CI/KR protection programs. DHS also sponsors a post-graduate-level program at the Naval Postgraduate School in homeland defense and security.

DHS will examine existing cyber security programs within the research and academic communities to determine their applicability as models for CI/KR protection education and broad-based research. These programs include:

- Co-sponsorship of the National Centers of Academic Excellence in Information Assurance Education (CAEIAE) program with the National Security Agency (NSA); and
- Collaboration with the National Science Foundation to co-sponsor 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 student bachelor's, master's, or doctoral study in information assurance in exchange for an equal amount of time spent working for the Federal Government.

DHS will ensure that the NCIP R&D Plan appropriately considers the human capital needs for protection-related R&D by incorporating analysis of the research community's future needs for advanced degrees in protection-related disciplines into the plan development process.

6.2.2.3 Continuing Education and Professional Competency

CI/KR protection involves many skills and professions that already feature education, training, and certification programs through professional organizations or government licensing. The CI/KR protection field also involves unique skills and professional expertise that have yet to incorporate such training and certification mechanisms into a nationwide system.

DHS encourages and, when appropriate, works with security partners to facilitate the development of continuing education, professional competency programs, and professional standards for areas requiring unique and critical CI/KR protection expertise. For example, DHS is collaborating with DOD to guide the development of a national certification program that includes a comprehensive set of information technology job skill standards for security professionals within the Federal Government and private industry. DHS will encourage and, when appropriate, facilitate the development of similar professional and surety standards for the remaining areas of unique and critical CI/KR protection expertise specified above.

6.2.3 Organizational Training and Exercises

Building and maintaining organizational and sector expertise requires comprehensive exercises to test the interaction between the NIPP and the NRP in the context of terrorist incidents, natural disasters, and other emergencies. Exercises are conducted by private sector owners and operators, and across all levels of government; they may be organized by these entities, on a sector-specific basis, or through three major national-level programs:

- **The National Exercise Program:** DHS provides overarching coordination for the National Exercise Program to ensure the Nation's readiness to respond in an all-hazards environment and to test the steady-state protection plans and programs put in place by the NIPP and their transition

to the incident management framework established in the NRP. Some examples of national exercises include TOPOFF and Ardent Sentry.

- **Homeland Security Exercises and Evaluation Program:** DHS also provides policy and guidance for designing, developing, conducting, and evaluating exercises to its security partners. HSEEP is a threat- and performance-based exercise program that includes a mix and range of exercise activities of varying degrees of complexity and interaction. HSEEP also includes a series of four reference manuals to help States and local jurisdictions establish exercise programs and design, develop, conduct, and evaluate exercises.
- **National Cyber Exercises:** DHS conducts exercises to identify, test, and improve coordination within the cyber incident response community, including Federal, State, local, tribal, and international government elements, as well as private sector corporations and coordinating councils. The Cyber Storm exercise conducted in February 2006 is an example of a national cyber exercise event.

DHS and the SSAs work together to ensure that these exercises include adequate testing of steady-state CI/KR protection

Pursuant to the National Exercise Plan, the **DHS Top Officials (TOPOFF)** national exercise series is a congressionally mandated, interagency program designed to strengthen the Nation's capacity to prevent, protect against, respond to, and recover from terrorist attacks involving WMD. This biennial exercise series is the cornerstone of the DHS National Exercise Program.

Ardent Sentry is an annual terrorism exercise focused on defense support to civil authorities that is jointly sponsored by the North American Aerospace Defense Command (NORAD) and the U.S. Northern Command (NORTHCOM). Ardent Sentry has been integrated with the DHS National Homeland Security Exercise Program and may be held concurrently with the TOPOFF exercises.

The **National Cyber Exercise** series is sponsored by the DHS National Cyber Security Division to strengthen preparedness, response, coordination, and recovery mechanisms to cyber incidents within international, Federal, and State governments, and in conjunction with the private sector. In accordance with congressional mandates to conduct exercises that test response to cyber attacks on critical infrastructures, the exercise meets HSPD-8, National Preparedness, requirements and is coordinated with the DHS National Exercise Program.

measures and plans, including information sharing; application of the NIPP risk management framework; and the ability for a protected core of life-critical CI/KR services, such as power, food and water, and emergency transportation, to withstand attacks or natural disasters and continue to function at an appropriate level.

DHS works with other security partners to facilitate the development of national standards, guidelines, and protocols for incident management training and exercises that include CI/KR protection evaluation to ensure that exercise programs include adequate testing of CI/KR steady-state protective measures and incident plans.

DHS will ensure that the NIMS Integration Center, which serves as the repository and clearinghouse for reports and lessons learned from actual incidents, training, and exercises, regularly compiles and disseminates information on CI/KR protection best practices.

6.2.4 Security Partner Role and Approach

Given the scope and nature of the education, training, and exercise needs related to CI/KR protection, the approach adopted must, to the greatest extent possible, leverage existing education, training, and exercise programs.

DHS will work through the NIPP partnership structure to provide initial training on the NIPP to introduce key public and private sector security partners to the plan's contents and requirements. DHS also will encourage and, where appropriate, facilitate specialized NIPP training, professional training, continuing education, and development of professional and personnel surety guidelines. It also will encourage academic and research programs, and coordinate with exercise managers on the design of exercises that test the interaction between the NIPP framework and the NRP.

The Interagency CI/KR Protection Training Task Force defines general training requirements and guides the development of national-level training standards associated with the NIPP. The SSAs and other Federal agencies should review and update existing CI/KR protection-related courses to align with the NIPP. Other security partners are encouraged to review existing courses to align with the NIPP or develop courses relevant to CI/KR protection needs within their jurisdiction. All security partners should work with DHS and the SSAs to identify and fill gaps in current training, education, and exercise programs for those specialized disciplines that are unique to CI/KR protection.

6.3 Conducting Research and Development and Using Technology

Federal agencies conduct R&D programs to help develop knowledge and technology that can be used by security partners to more effectively mitigate the risk to CI/KR. Congress has provided for liability protections under the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act) that serve to encourage technology use by CI/KR security partners.

6.3.1 R&D Programs

In the near term, risk-based priorities are designed to address the challenges posed by the limited resources available to meet all CI/KR protection needs by allocating protection resources where they can best mitigate risk. In the long term, R&D holds the key to more effective and cost-efficient CI/KR protection through advances in technology. R&D programs work to improve all aspects of CI/KR protection—from detection of threats, through protection and performance measures, to inherently secure advanced infrastructure designs. Because owners and operators play a major role in CI/KR protection, research programs that support the NIPP must find effective ways to consider the perspectives of sector professional associations, sector councils, and other sources that understand owner and operator technology needs.

Unique R&D needs associated with CI/KR protection include:

- Conducting development, or re-design, of technology-based equipment to significantly lower the costs of existing capabilities rather than improving technical performance, so that security partners with limited budgets can afford state-of-the-art solutions;
- Researching issues, such as resiliency and protection in building design, that affect all CI/KR and can result in solutions that can provide benefits across sectors if implemented; and
- Focusing research on the implementation and operational aspects of technology used for CI/KR protection to provide resources that can help inform technology investment decisions, such as technical evaluation of security equipment or technology clearing house information.

R&D supporting the NIPP includes planning and program activities undertaken in three general areas: (1) the NCIP R&D Plan, (2) the Federal Plan for Cyber Security R&D, and (3) R&D and planning efforts conducted by the SSAs and other agencies in support of the requirements set forth in the President's Physical and Cyber CI/KR Protection Strategies.

Additionally, Technology Pilot Programs are used to develop solutions to CI/KR protection problems with technologies that have passed the research stage and require demonstration in operational use. Each of these is discussed in the sections that follow. Appendix 6 provides more details on specific R&D plans and programs supporting CI/KR protection.

6.3.2 The SAFETY Act

As part of the Homeland Security Act, Public Law 107-296, Congress enacted the SAFETY Act, which creates liability protections for sellers of qualified anti-terrorism technologies. The SAFETY Act provides incentives for the development and deployment of anti-terrorism technologies by limiting liability through a system of risk and litigation management. The purpose of the SAFETY Act is to ensure that the threat of liability does not deter potential sellers of anti-terrorism technologies from developing, deploying, and commercializing technologies that could save lives. The SAFETY Act gives liability protection to both sellers of qualified anti-terrorism technology and their customers, and applies to all types of enterprises that develop, sell, or use anti-terrorism technologies.

The SAFETY Act applies to a broad range of technologies, including products, services, and software, or combinations thereof, as well as technology firms and providers of security services. The SAFETY Act protects those businesses and their customers and contractors by providing a series of liability protections if their products or services are found to be effective by the Secretary of Homeland Security. Additionally, if the Secretary certifies the technology under the SAFETY Act (i.e., that the technology actually performs as it is intended to do and/or conforms to certain seller specifications), the seller is afforded a complete defense in litigation related to the performance of the technology in preventing, detecting, or deterring terrorist acts or deployment to recover from one. Those technologies that have been “certified” are placed on an Approved Product List for Homeland Security that is published at www.safetyact.gov.

A clear benefit of the SAFETY Act is that a cause of action may be brought only against the seller of the Qualified Anti-Terrorism Technology and may not be brought against the buyer(s), their contractors, or downstream users of the Qualified Anti-Terrorism Technology, or against the seller’s suppliers or contractors. This stipulation includes CI/KR owners and operators.

CI/KR facility owners and operators are encouraged to examine the SAFETY Act closely because: (1) CI/KR owners (if purchasers of qualified technologies) will enjoy the

liability protections that flow from using qualified SAFETY Act technologies, and (2) CI/KR owners will also have a level of assurance that the qualified products/services they are utilizing have been vetted by DHS. Lower liability insurance burdens for those using qualified technologies are another potential outcome.

In these ways, the SAFETY Act is a valuable tool that can enhance the ability of owners and operators to protect our Nation’s CI/KR.

6.3.3 National Critical Infrastructure Protection R&D Plan

As directed by HSPD-7, the Secretary of Homeland Security works with the Director of the OSTP, Executive Office of the President, to develop the NCIP R&D Plan as a vehicle to support implementation of CI/KR risk management and supporting protective activities and programs.

The NCIP R&D Plan provides the focus and coordination mechanisms required to achieve the vision provided in the President’s Physical and Cyber CI/KR Protection Strategies. That vision calls for a “systematic national effort to fully harness the Nation’s research and development capabilities.” The R&D planning process is designed to address common issues faced by the various sector security partners and ensure a coordinated R&D program that yields the greatest value across a broad range of interests and requirements. The plan addresses both physical and cyber CI/KR protection. The planning process also provides for the revision of research goals and priorities over the long term to respond to changes in the threat, technology, environment, business continuity, and other factors.

DHS and OSTP coordinate with Federal and private sector security partners, including academic and national laboratory representatives, during the R&D planning cycle. The interagency process used to develop and coordinate this plan is managed through the Infrastructure Subcommittee of the National Science and Technology Council (NSTC), which is co-chaired by DHS and OSTP. The SSAs are responsible for providing input into the plan after coordination with sector representatives and experts through such bodies as the SCCs and GCCs.

The NCIP R&D Plan articulates strategic R&D goals and identifies the R&D areas in which advances in CI/KR protection must be made. The plan also provides an R&D technology roadmap against which current and planned risk management and CI/KR protection R&D initiatives can be evaluated to define a program of CI/KR protection-related technology

development. The goals, R&D areas, and technology roadmap contained in the NCIP R&D Plan are discussed in the following subsections. A final subsection describes coordination of SSP R&D planning with the NCIP R&D Plan.

6.3.3.1 CI/KR Protection R&D Strategic Goals

The NCIP R&D planning process identifies three long-term, strategic R&D goals for CI/KR protection:

- A common operating picture architecture;
- A next-generation Internet architecture with designed-in security; and
- Resilient, self-diagnosing, self-healing systems.

The strategic goals are used to guide Federal R&D investment decisions and also to provide a coordinated approach to the overall Federal research program. The DHS Science and Technology (S&T) Directorate and OSTP will work with the OMB to use the R&D Plan as a decisionmaking tool for evaluation of budget submissions across Federal agencies. These goals also help guide programs of research performers who receive Federal grants and contracts.

6.3.3.2 CI/KR Protection R&D Areas

R&D development projects for CI/KR protection programs fall into nine R&D areas or themes that cut across all CI/KR sectors:

- Detection and sensor systems;
- Protection and prevention systems;
- Entry and access portals;
- Insider threats;
- Analysis and decision support systems;
- Response, recovery, and reconstitution tools;
- New and emerging threats and vulnerabilities;
- Advanced infrastructure architectures and systems design; and
- Human and social issues.

Organizing research in these areas enables the development of effective solutions that may be applied across sectors and disciplines. These themes also provide an organizing framework for SSA use during the development of R&D requirements for their respective sectors, which will be reflected in the SSPs. These requirements specify the capabilities each sector needs to satisfy CI/KR protection needs. By incorpor-

ating these requirements into the NCIP R&D Plan, OMB is better able to ensure that agency R&D budget requests are aligned with the National R&D Plan for CI/KR Protection.

6.3.3.3 CI/KR Protection R&D Roadmap

The NCIP R&D technology roadmap provides a way for Federal R&D managers such as DHS, OSTP, OMB, and the SSAs, to coordinate CI/KR protection R&D across NIPP security partners. This roadmap provides a systematic approach to identify current technology investment plans, determine gaps, and outline the timeline for addressing unmet requirements. It also provides a systematic way to determine interrelationships among other R&D programs, both public and private, and ensures synchronization with the SSA R&D plans contained in the SSPs.

6.3.3.4 Coordination of NCIP R&D Plan With SSP R&D Planning

Each SSP will include a component on sector-specific CI/KR protection R&D that explains how the sector will strengthen the linkage between sector-specific and national R&D planning efforts, technology requirements, current R&D initiatives, gaps, and candidate R&D initiatives. This component of the SSP explains the process for:

- **Sector Technology Requirements:** Identifying and providing a summary of sector technology requirements, and communicating them to the DHS S&T Directorate/OSTP for inclusion in the NCIP R&D Plan on an annual basis;
- **Current R&D Initiatives:** Annually soliciting a listing of current Federal R&D initiatives from the DHS S&T Directorate/OSTP that have the potential to meet sector CI/KR protection challenges, and providing a description of how this listing will be analyzed to indicate which initiatives have the greatest potential for a positive impact;
- **Gaps:** Conducting an analysis of the gaps between the sector's technology needs and current R&D initiatives from the DHS S&T Directorate/OSTP; and
- **Candidate R&D Initiatives:** Determining which candidate R&D initiatives are most relevant for the sector and how these will be summarized and reported to all appropriate stakeholders.

Each SSA will coordinate the development of the sector R&D planning component of their SSP so that these documents reflect the SSA's sector-level R&D investment priorities. Coordination between DHS/S&T and the sectors through the SSAs, GCCs, and SCCs ensures that the R&D information in the SSP will be consistently documented and prioritized.

6.3.4 Cyber Security R&D Planning

The Cyber Security R&D Act authorized a multi-year effort to create more secure cyber technologies, to expand cyber security R&D, and to improve the cyber security workforce. To further address cyber R&D needs, OSTP has established the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG) under the NSTC. The CSIA IWG is jointly chartered by NSTC's Subcommittee on Networking and Information Technology R&D and the Subcommittee on Infrastructure. DHS co-chairs this interagency working group, which includes participation by Federal departments and agencies, as well as offices in the White House. The interagency working group coordinates policy, programs, and budgets for cyber security and information assurance R&D.

The CSIA IWG develops the Federal Plan for Cyber Security R&D, which includes near-term, mid-term, and longer term cyber security research efforts, as called for in the National Strategy to Secure Cyberspace and as directed in HSPD-7. Specific research efforts include programs to improve the security of fundamental protocols (such as Internet Protocol Version 6) and authentication technologies.

DHS identifies critical cyber R&D requirements for incorporation into this national R&D planning effort. DHS and OSTP also facilitate communications between the public and private research communities and the security community to ensure that emerging technologies are periodically reviewed by the appropriate body within the NSTC to determine possible homeland security and cyber security applications or appropriateness for inclusion in the Federal research portfolio.

6.3.5 Other R&D That Supports CI/KR Protection

Other R&D efforts that may support CI/KR protection are conducted by the SSAs and other Federal agencies. These programs address the research requirements set forth in the President's Physical and Cyber Security CI/KR Protection Strategies, which call for:

- Ensuring the compatibility of communications systems with interoperability standards;
- Exploring methods to authenticate and verify personal identity;
- Coordinating the development of CI/KR protection consensus standards; and
- Improving technical surveillance, monitoring, and detection capabilities.

For example, the Technical Support Working Group is the U.S. national forum that identifies, prioritizes, and coordinates interagency and international R&D requirements for combating terrorism. The Technical Support Working Group rapidly develops technologies and equipment to meet the high-priority needs of the combating terrorism community, including efforts that can contribute to CI/KR protection, and addresses joint international operational requirements through cooperative R&D with major allies.

Other examples of R&D that may support CI/KR protection include the SAFECOM program conducted by the DHS S&T Directorate Office of Interoperability. This program serves as the Federal umbrella to promote and coordinate initiatives between State, local, and tribal entities to develop interoperable wireless communications. SAFECOM's primary role is to work with Federal agencies and public safety personnel to define requirements and to create standards, models, and solutions to help meet those requirements.

DHS also conducts cooperative R&D programs with other Federal agencies related to authentication and verification of personal identity for the CI/KR protection workforce, and works with the American National Standards Institute and the National Institute of Standards and Technology (NIST) through the Homeland Security Standards Panel to help coordinate the development of consensus standards that support CI/KR protection.

6.3.6 Technology Pilot Programs

DHS identifies CI/KR protection needs common to certain types of assets or geographical areas while conducting site assistance, buffer zone protection visits, and other vulnerability and risk assessments. In some situations, a technological solution may be the best approach to addressing such needs. If a development program is required to create or test a potential technological solution, the DHS S&T Directorate works closely with relevant security partners to implement a technology pilot program. In some cases, this involves working with the DHS Office of Grants and Training (G&T) to identify funds and specialized training. If the pilot program is successful, the technological solutions are then implemented in other locations where similar needs exist. The following technology pilot programs illustrate some of the important capabilities that these programs can offer to security partners:

- **The National Capital Region Rail Security Corridor Pilot Project:** This project is designed to address security challenges surrounding high-risk rail infrastructure and freight traffic transiting major urban areas while maintaining fluid rail operations and meeting the needs of local law enforcement, first-responders, and the Federal Government.
- **The Constellation Automated Critical Asset Management System (Constellation/ACAMS):** This project is being developed through a partnership between DHS, the California Office of Homeland Security, and the City and County of Los Angeles. It includes a reporting capability to answer both local and national data calls on CI/KR, including information on location, size, key contacts, types of hazardous materials on site, and vulnerability assessments. It also provides for the automatic generation of BZPPs and pre-incident operational plans for local police and first-responder use in real time.
- **Coastal Surveillance Prototype Test Beds:** This iterative project is designed to provide advanced port and coastal surveillance systems. Test bed projects have been conducted in South Florida in the Port Everglades, Miami, and Key West areas, and at the Hampton Roads Sector Command Center in Virginia. Additional efforts are planned for other areas, such as Mayport, FL, and Seattle, WA.

6.4 Building, Protecting, and Maintaining Databases, Simulations, and Other Tools

Many data systems, databases, models, simulations, decision support systems, and similar information tools currently exist or are under development to enable the execution of national risk management for CI/KR.

To keep pace with the constantly evolving threat, technology, and business environments, these tools must be updated and, in some cases, new tools must be developed. Sensitive information associated with these tools must be appropriately protected. Priority efforts in this area will be focused on updating and improving key databases, developing and maintaining simulation and modeling capabilities, and coordinating with security partners on databases and modeling.

6.4.1 National CI/KR Protection Data Systems

HSPD-7 directs the Secretary of Homeland Security to implement plans and programs that identify, catalog, prioritize, and protect CI/KR in cooperation with all levels

of government and private sector entities. Data systems currently provide the capability to catalog, prioritize, and protect CI/KR through such functions as:

- Maintaining an inventory of asset information and estimating the potential consequences of an attack or incident (e.g., the NADB);
- Storing information related to terrorist attacks or incidents (e.g., the National Threat and Incident Database);
- Analyzing dependencies and interdependencies (e.g., the NISAC);
- Managing the implementation of various protective programs (e.g., the BZPP Request Database); and
- Providing the continuous maintenance and updating required to enable data in these systems to reflect changes in actual circumstances.

Properly maintaining systems with current and useful data involves long-term support, coordination, and resource commitments by DHS, the SSAs, the States, private sector entities, and other security partners. Important aspects of the support, coordination, and resource commitments required over the long term to sustain the NIPP include:

- **Need for Information Protection:** Data accuracy and currency for CI/KR protection is dependent upon the ability of the various security partners to keep their databases and data systems current. Over the long term, the level of cooperation and commitment needed for this must be sustained by a trusted working relationship between various security partners. This requires that information regarded as sensitive by providers be protected from unauthorized access, use, or disclosure. Data content, accuracy, and currency must also be protected from tampering or other corruption.
- **Durable Information:** The complexity, scope, and magnitude of the U.S. CI/KR require reliance on multiple data sources that are acquired over long periods of time. As a result, information pertaining to the characteristics and quality of the data must be provided along with the actual data from each source. This requires the use of a common and standardized format, data scheme, and categorization system (i.e., taxonomy) that is viable over the long term. DHS and the SSAs are responsible for working together to establish and utilize the appropriate data collection format. The DHS taxonomy is the foundation for multiple DHS programs that focus on CI/KR information, such as the

NADB and the National Threat Incident Database. This taxonomy provides the foundation for a national-level information scheme.

- **Recurring Nature of Information Needs:** The process of information identification and additional data collection represents a recurring need. Data requirements and availability are continually reassessed based on the current threat environment, analyses to identify gaps, or other factors. Focused data calls to specific sectors or locales, in coordination with the SSAs and the States, as appropriate, may be required to fill identified information gaps. This imposes a continuing need for resources to build and update the system over the long term.

6.4.2 Simulation and Modeling

A number of security partners make use of simulations and modeling to comprehensively examine the potential consequences from terrorist attack, natural disasters, and manmade accidents that impact CI/KR, including the effects of sector and cross-sector dependencies and interdependencies. Continuous maintenance and updating are required for these tools to produce reliable projections. Over the long term, new tools are needed to address fundamental changes due to factors such as technology, threats, or the business environment.

The DHS Preparedness Directorate is the lead for modeling and simulation capabilities regarding CI/KR protection. In this capacity, the DHS Preparedness Directorate will:

- Coordinate with the DHS S&T Directorate on requirements for the development, maintenance, and application of research-related modeling capabilities for CI/KR protection;
- Specify requirements for the development, maintenance, and application of operations-related modeling capabilities for CI/KR protection in coordination with the DHS S&T Directorate and the SSAs, as appropriate;
- Coordinate with the SSAs that have relevant modeling capabilities to develop appropriate mechanisms for the development, maintenance, and use of such for CI/KR protection as directed by HSPD-7;
- Familiarize the SSAs and other security partners with the availability of relevant modeling and simulation capabilities through training and exercises;

- Work with end-users to design operations-related tools that provide maximum utility and clarity for CI/KR protection activities in both emergencies and routine operations;
- Work with end-users to design appropriate information protection plans for sensitive information used and produced by CI/KR protection modeling tools;
- Provide guidance on the vetting of modeling tools to include the use of private sector operational, technical, and business expertise where appropriate; and
- Review existing private sector modeling initiatives and opportunities for joint ventures to ensure that DHS and its security partners make maximum use of private sector modeling capabilities.

The NISAC, within DHS/OIP, provides advanced modeling and simulation capabilities for the analysis of CI/KR interdependencies, vulnerabilities, and other complex interactions. In accordance with the Homeland Security Act, DHS/OIP manages the development, maintenance, and use of relevant modeling capabilities by NISAC for CI/KR protection. NISAC technical capabilities include: data analysis; infrastructure and infrastructure interdependency modeling and simulation; decision support methodologies and tools; risk analysis; and knowledge management system design, development, and management.

NISAC activities fall into five broad categories: (1) analysis on an as-needed basis with quick turnaround time; (2) detailed analysis of infrastructure and its interdependencies; (3) risk-based decision methodology assessment, development, and implementation; (4) development of the tools and data necessary to perform and improve infrastructure analyses; and (5) support to DHS to define direction for applied R&D in support of next-generation infrastructure analysis tools.

6.4.3 Coordination With Security Partners on Databases and Modeling

Integrating existing databases into DHS databases, such as the NADB, not only reduces duplication of effort, but also ensures that available data are consistent, current, and accurate, and provide users with a consolidated picture across all CI/KR sectors. However, this approach is effective only if the source information is protected and maintained properly. Maintaining a current and useful database involves the support, coordination, and commitment of the SSAs, private

sector entities, and other security partners. Because the most current and accurate CI/KR-related data are best known by owners and operators, the effectiveness of the effort depends on all security partners keeping their databases and data systems current.

As the responsible agent for the identification of assets and existing databases for their sectors, the SSAs will:

- Outline in their SSPs the sector plans and processes for the database, data system, and modeling and simulation development and updates;
- Work with sector security partners to facilitate the collection and protection of accurate information for database, data system, and modeling and simulation use;
- Specify the timelines and milestones for the initial population of CI/KR databases; and
- Specify a regular schedule for maintenance and updating of the databases.

DHS will work with the SSAs and other security partners to:

- Identify databases and other data services that will be integrated with CI/KR protection databases and data systems;
- Facilitate the actual integration of supporting databases or importation of data into CI/KR protection databases and data systems, using a common and standardized format, data scheme, and categorization system or taxonomy specified by DHS in coordination with the SSAs; and
- Define the schedule for importing data and databases into such systems as the NADB.

6.5 Continuously Improving the NIPP and the SSPs

The NIPP uses the SCCs, GCCs, and the Government and Private Sector Cross-Sector Councils as the primary forums for coordination of policy, planning, training, and other requirements needed to ensure efficient implementation and ongoing management and maintenance of the NIPP and the SSPs.

6.5.1 Management and Coordination

DHS/OIP is the Federal executive agent for NIPP management and maintenance.

The NIPP is a multi-year plan describing mechanisms for sustaining the Nation's steady-state protective posture. The NIPP and its component SSPs include a process for annual review; periodic interim updates as required; and regularly scheduled partial reviews and re-issuance every 3 years, or more frequently, if directed by the Secretary of Homeland Security.

DHS/OIP will oversee the review and maintenance process for the NIPP; the SSAs, in coordination with the GCCs and SCCs, will establish and operate the mechanism(s) necessary to coordinate this review for their respective SSPs. The NIPP and SSP revision processes will include developing or updating any documents necessary to carry out NIPP activities. The NIPP will be reviewed at least annually to:

- Ensure that the NIPP framework is capable of measuring accomplishments in support of CI/KR protection goals and objectives and supporting the overall national approach to the homeland security mission;
- Ensure that the plan adequately reflects the organization of DHS, the SSAs, and the Federal budget process;
- Ensure that the NIPP is consistent with those Federal plans and activities that it directly supports;
- Adjust practices and procedures called for in the NIPP based on changes in the national risk management environment;
- Incorporate lessons learned and best practices from day-to-day operations, exercises, and actual incidents and alerts; and
- Reflect progress in the Nation's CI/KR protection, as well as changes to national priorities and guidance, critical tasks, sector organization, or national capabilities.

As changes are warranted, periodic updates to the NIPP will be issued. Types of developments that merit a periodic update include new laws, executive orders, Presidential directives, or regulations, and procedural changes to NIPP activities based on real-world incidents or exercise experiences.

6.5.2 Maintenance and Updating

The following paragraphs establish the procedures for posting interim changes and periodic updating of the NIPP:

- **Types of Changes:** Changes include additions of new or supplementary material and deletions. No proposed change should contradict or override authorities or other plans contained in statute, executive order, or regulation.

- **Coordination and Approval:** While DHS is the Federal executive agent for NIPP management and maintenance, any Federal department or agency with assigned responsibilities under the NIPP may propose a change to the plan. DHS is responsible for coordinating the review and approval of all proposed modifications to the NIPP with SSAs and other security partners, as appropriate. Policy changes will be coordinated and approved through the Homeland Security Council policy process.
- **Notice of Change:** DHS will issue an official Notice of Change for each interim revision to the NIPP. After publication, the modifications will be considered part of the NIPP for operational purposes pending a formal revision and re-issuance of the entire document. Interim changes can be further modified or updated using this process.
- **Distribution:** DHS will distribute Notices of Change to SCCs, GCCs, and other security partners. Notices of Change to other organizations will be provided upon request.
- **Re-Issuance:** DHS will coordinate full reviews and updating of the NIPP every 3 years, or more frequently, if the Secretary deems necessary. The review and updating will consider lessons learned and best practices identified during implementation in each sector and will incorporate the periodic changes and any new information technologies. DHS will distribute revised NIPP documents for inter-agency review and concurrence through the Homeland Security Council process.

The SSAs, in coordination with the GCCs and SCCs, will establish and operate the mechanism(s) necessary to coordinate SSP maintenance and update in accordance with the process established for the NIPP.