Appendix 6: Research and Development to Improve CI/KR Protection Capabilities

This appendix provides additional details on R&D programs and initiatives supporting the NIPP. It also includes details of R&D planning and programs undertaken in three areas: (1) those conducted under the NCIP R&D Plan; (2) those conducted by the SSAs and other agencies in support of requirements set forth in the President's physical and cyber security CI/KR strategies; and (3) those classified as Technology Pilot Programs, which develop technology-based solutions using more mature technology.

6.1 The 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 annual NCIP R&D Plan.

The NCIP R&D Plan uses the three-step approach described below to direct the development of CI/KR protection-related technologies to meet existing and future requirements:

Step 1: Identify CI/KR Protection R&D Strategic Goals and Objectives

The NCIP R&D planning process identifies three long-term strategic goals and provides direction to the R&D community through a prioritized CI/KR protection agenda:

- **A common operating picture architecture** that will integrate CI/KR monitoring and support systems with data collection, processing, analysis, modeling, and simulation, including interdependencies and visualization capabilities, to provide real-time analysis and reports on the status and security of the Nation's CI/KR;

- **A next-generation Internet architecture** with designed-in security that is more secure than the existing Internet. The architecture will incorporate security and protection measures at all levels, from the basic hardware components through all layers of software, as an explicit design feature of this new network, rather than adding it later as a post-development patch; and
- **Resilient, self-diagnosing, self-healing systems** that, if attacked or damaged, can manage or contain the extent of the damage, continue to provide critical services, and adapt and self-heal damaged areas.

Step 2: Identify CI/KR Protection R&D Themes

The S&T needs for CI/KR protection programs fall into nine topical themes, or R&D areas, that cut across all CI/KR sectors:

- **Detection and Sensor Systems:** Selection, placement, and integration of systems to detect WMD intrusion, small arms, intent, humans (actors and victims), and disease outbreak. The research plans for certain sensors and detectors reside within several R&D communities, specifically for chemical, biological, radiological, nuclear, and explosive agents. The standards community also has a role in fostering interoperable sensor systems and establishing performance specifications.
- **Protection and Prevention Systems:** Devices, methods, and processes that prevent damage, disruption, or destruction of CI/KR. This theme involves layers of defensive measures that deter attackers, prevent entry, inhibit the use of weapons, and harden infrastructure.
- **Entry and Access Portals:** Devices, systems, and methods that control access to CI/KR. The types of portals include physical entryways and communications nodes. The objects of interest passing through portals include people, vehicles, goods, cargo and freight, electronic information, and communications. The enabling technologies include full life-cycle identity management, including biometric identification and automated identification strong authentication methods such as biometrics, radio frequency tags, sensor data, and x-ray interrogation systems.
- **Insider Threat Detection:** Profiling, detection, anticipation, and monitoring of activities of trusted persons or automated entities with access to a critical asset, system, or network, whether central or distributed. This theme focuses on detecting malicious intent, monitoring activities to identify anomalies and early indicators, and prevention and protection through real-time auditing of systems and layered measures to prevent malicious actions.
- **Analysis and Decision Support Systems:** Modeling, simulation and analysis, and decision support tools to analyze the complex systems and situations found in terrorist attack scenarios, including dependencies and interdependencies among sectors. This theme is of ubiquitous importance across sectors because CI/KR assets, systems, and networks are highly interdependent. Systems to be developed include risk-based prioritization and investment strategy aids; vulnerability assessment tools; modeling and simulation of sector operations, interconnectivity, and the consequences of attacks; and response planning tools to simulate scenarios and evaluate candidate responses.
- **Response, Recovery, and Reconstitution Tools:** Systems, devices, and processes that support first-responders and those building temporary and permanent replacement of damaged infrastructure, as well as the planning systems for all such efforts. Associated technologies include equipment to detect victims and assess safety hazards, simulation tools for response planning and training, and self-recovery design for cyber systems.
- **Emerging Threats and Vulnerabilities Analysis Aids:** Methods and processes that enable early discovery of emerging threats and vulnerabilities or the potential of adversaries to present new threats. Many emerging physical threats relate to changes in the lethality, detectability, or resistance to countermeasures of WMD agents. New cyber threats include those with the capability to attack a wide range of networks; new health threats include the emergence of infectious diseases, such as pandemic flu.

- **Advanced Infrastructure Architectures:** Use of new technology and associated designs that address current and future infrastructure needs with replacements that are inherently more secure (e.g., Internet contingency and SCADA system security). Greater inherent security can rely on automatic responses to attacks, self-healing features, and co-design of physical and cyber components that can prevent, respond to, or recover from attacks more quickly than current systems. Such improvements can have important dual-use benefits, with systems better able to respond to minor, but frequent, accidental events that degrade performance.
- **Human and Social Issues:** Research into behavioral issues related to victim response and CI/KR owner/operator actions to enhance understanding and decisionmaking during a terrorist event. The focus areas for this theme include coordination among government and private sectors, user-centered designs, the resiliency of commercial enterprises and the economy, and risk communications and management.

Step 3: Establish the NCIP R&D Technology Roadmap

The final step of the planning process involves the development of the NCIP R&D Technology Roadmap. Patterned after the technology roadmaps in wide use across U.S. industry, the roadmap provides a way for Federal managers such as DHS, OSTP, OMB, and the SSAs to coordinate infrastructure protection R&D, as well as a systematic approach to identify current technology investment plans, determine gaps, and outline the timeline for addressing unmet requirements.

6.2 Other R&D That Supports CI/KR Protection

Other R&D efforts, developed in accordance with the requirements set forth in the President's Physical and Cyber CI/KR Protection Strategies, that will be used to support CI/KR risk mitigation are discussed in this section. These requirements include:

- Ensure compatibility of communications systems with interoperability standards;
- Explore methods to authenticate and verify personal identity;
- Coordinate development of CI/KR protection consensus standards; and
- Improve technical surveillance, monitoring, and detection capabilities.

Examples of programs in each of these areas are discussed below to illustrate the potential benefits of such programs to security partners.

6.2.1 Ensure Compatibility of Communications Systems With Interoperability Standards

SAFECOM, a program in the DHS S&T Directorate, serves as the Federal umbrella to promote and coordinate initiatives among State, local, and tribal entities to improve first-responder communications through more effective and efficient interoperable wireless communications. SAFECOM's primary role is to work with Federal agencies and public safety personnel to define requirements and create standards, models, and solutions to help meet those requirements.

SAFECOM's role in standards development is to:

- Support existing or, where necessary, establish a voluntary consensus process that meets the current security environment, identifies and implements the needs and requirements of public safety, and maximizes flexibility and innovation; and
- Develop near-term tools that can maximize the efficiency of public safety technology, such as recommended models for statewide planning, criteria for creating governing bodies, standard operating procedures, grant guidance, and communications-specific exercise methodologies.

The following are key characteristics of SAFECOM's approach to facilitating the development of national voluntary consensus standards for public safety interoperable communications:

- Implements a practitioner-driven approach;
- Applies a comprehensive framework that utilizes a structured life-cycle approach that employs continuously evolving common grant guidance to assist communities in planning and implementing interoperability solutions;
- Integrates new and legacy systems using a "system of systems"; and
- Establishes industry and government partnerships.

6.2.2 Explore Methods to Authenticate and Verify Personal Identity

In coordination with a number of Federal agencies, DHS funds several R&D programs related to the authentication and verification of personal identity for the CI/KR workforce. Examples include research into the protection of physical infrastructure by authentication of network users, recommendations from the private security guard industry on legislative measures needed to achieve progress in the area of personnel surety (including enhanced capabilities for background checks on personnel with critical access), and advances in basic research. Another example is the DHS Office of National Capital Region Coordination initiative to establish partnerships with Federal, State, and local governments, as well as private sector organizations, to provide strong, machine-readable identity authentication for CI/KR response/support personnel in its region.

6.2.3 Coordinate Development of CI/KR Protection Consensus Standards

DHS worked with the American National Standards Institute and NIST to establish a Homeland Security Standards Panel that has been coordinating the development of consensus standards among the 280 different standards development organizations. An important product of this work was the standards supporting HSPD-12, which mandates reliable forms of identification issued by the Federal Government, as well as the identity-proofing guidance supporting the eAuthentication initiative.

6.2.4 Improve Technical Surveillance, Monitoring, and Detection Capabilities

Advances in surveillance, monitoring, and detection increase the Nation's ability to find threats in the making rather than responding to an attack after the fact. From an R&D perspective, advanced processing of digital video and other data collection methods is important in providing information to responsible security forces in a way that is reliable, practical, and fast. In cooperation with the United Kingdom, U.S. expertise has been brought to bear on reducing the amount of data that needs to be transmitted by extracting out only that information required for sophisticated analysis. Massive data storage capacity that is small and affordable is also nearing readiness for the market as a result of R&D investments by the government and private sectors. These advances make better use of the data collection capacity readily available, while providing information to security officials in a more actionable, focused manner.

In addition, the integration of biological, chemical, and radiological environmental and public health surveillance monitoring and detection capabilities, coupled with analysis tools, provides additional situational awareness and improves the ability of decisionmakers to determine appropriate courses of action in a WMD event.

6.3 Technology Pilot Programs

DHS identifies CI/KR protection needs common to certain types of assets, sectors, or high-risk jurisdictions in the course of conducting site assistance visits, buffer zone protection visits, and other vulnerability and risk assessments. In some situations, a technological development program is required to create or test the appropriate technological solution, and

the DHS S&T Directorate works closely with other relevant security partners to conduct a Technology Pilot Program. If the pilot program is successful, the technological solutions are then implemented in other locations where similar needs exist. The following descriptions of Technology Pilot Programs provide good examples of the capabilities that these programs can offer security partners:

6.3.1 National Capital Region Rail Security Corridor Pilot Project

This pilot project is designed to meet the needs of local law enforcement, first-responders, and the Federal Government while supplementing the existing security measures of freight rail operations in the Washington, DC, area. This pilot project seeks to address security challenges surrounding rail infrastructure and freight traffic through large cities while maintaining fluid rail operations. The pilot project components include a "virtual security fence" consisting of approximately 200 high-resolution fixed cameras, the use of radio frequency identification scanners, and virtual gates for chemical and radiological detection. Data from the fence and the gates will be encrypted and transmitted simultaneously to multiple locations, such as the U.S. Capitol Police, U.S. Secret Service, the rail corridor's owner/operator, and other applicable Federal or local agencies.

6.3.2 Constellation Automated Critical Asset Management System

Constellation/ACAMS, developed through a partnership between DHS and the City and County of Los Angeles as part of the Operation Archangel CI/KR protection program, encompasses automated systems, tools, resources, and related training to enable the protection of CI/KR located in major urban areas. Constellation/ACAMS enables planning for, responding to, and recovering from catastrophic incidents. As such, it focuses on the unique requirements and information needs of first-responders. It possesses a complete reporting capability to answer both local and national data calls on critical assets, including information on location, size, key contacts, types of hazardous materials on site, and vulnerability assessments. It also provides for the automatic generation of BZPP and pre-incident operational plans for local police and first-responder use.

6.3.3 South Florida Coastal Surveillance Prototype Test Bed

The DHS S&T Directorate and the USCG planned and funded the South Florida Coastal Surveillance Prototype Test Bed, a port and coastal surveillance prototype in the Port Everglades, Miami, and Key West areas. The evolutionary prototype provides an initial immediate coastal surveillance capability in a high-priority area that:

- Offers the means to develop and evaluate a concept of operations in a real-world environment;
- Implements and tests interoperability among DHS and DOD systems and networks such as the U.S. Navy/USCG Joint Harbor Operations Center;
- Tests and evaluates systems and operational procedures; and
- Becomes the design standard for follow-on systems in other areas and integration with wider area surveillance systems.