Public Health & Healthcare

Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (Redacted)

May 2007

Homeland Security

Department of Health and Human Services

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Office of the Assistant Secretary for
Public Health Emergency Preparedness
Washington, D.C. 20201

April 30, 2007

Subject: *Healthcare and Public Health Government Coordinating Council Concurrence*

The Healthcare and Public Health (HPH) Sector Government Coordinating Council (GCC) is pleased to have participated in the review of final revisions to the 2006 Healthcare and Public Health Sector-Specific Plan (SSP). This plan provides the overarching framework for integrating the healthcare and public health sector critical infrastructure and key resource protection efforts into a unified program coordinated by the Department of Homeland Security (DHS) as directed by the National Infrastructure Protection Plan (NIPP) and HSPD-7. Through a developing relationship and direct collaboration, the HPH Sector Coordinating Council (SCC) and the Healthcare Sector Coordinating Council (HSCC) were able to develop a plan that lays out a logical and workable framework for a strong public/private partnership that will help better secure the HPH Sector and the country as a whole.

The Federal, State, Local and Tribal members that compose the Healthcare and Public Health Sector GCC support the concepts and processes described in the 2006 HPH SSP and are committed to working with DHS and other sector security partners to help achieve the goals established in the plan. This work will be appropriate and consistent with the authorities, resources, and programs specific to each of the departments and agencies which compose the HPH Sector GCC.

Recognizing that the HPH SSP is intended to be a living document, the HPH Sector GCC also commits to continuing to work with DHS and the HSCC to ensure that the plan is updated as needed. This collaborative effort will enable us to better focus the limited resources available for critical HPH infrastructure protection in the most effective and efficient manner.

As approved by those on the HPH Sector GCC who participated in the review of the final 2006 HPH SSP, I, R. Tom Sizemore, being the HHS Sector Specific Agency representative, am pleased to concur on this version of the HPH SSP on behalf of the HPH Sector GCC.

This signed "Letter of Agreement" from the HPH Sector GCC indicates concurrence with the final 2006 HPH SSP.

R. Tom Sizemore, III, MD
Principal Deputy Director, Preparedness & Emergency Operations
Office of Public Health Emergency Preparedness

Department of Health and Human Services

Healthcare Sector Coordinating Council Letter of Acknowledgment

The Healthcare and Public Health Sector-Specific Plan (SSP), in conjunction with the National Infrastructure Protection Plan (NIPP), provides a structure for the integration of healthcare functions and critical infrastructure and key resources (CI/KR) protection efforts. The NIPP provides an overall framework for integrating national programs and activities currently underway in the sector, as well as new and developing CI/KR protection efforts. The Healthcare and Public Health SSP describes a process for a collaborative effort among the private sector; local, State and tribal governments; nongovernmental organizations; and the Federal government. This collaboration will result in the prioritization of protection initiatives and investments across the Healthcare and Public Health sector. This prioritization helps ensure that government resources are applied where they offer the most benefit for mitigating risk by lowering vulnerabilities, deterring threats, and minimizing the consequences of attacks and other incidents. The Healthcare and Public Health SSP encourages a similar allocation of resources within the private sector. For the healthcare sector in particular, it is critically important that the NIPP and Healthcare and Public Health SSP be coordinated with the National Response Plan.

By signing this letter, the members of the Healthcare Sector Coordinating Council acknowledge that they:

- Will continue to work with the Departments of Health and Human Services and Homeland Security and other security partners to develop the SSP and to integrate strategies for protecting and preserving the healthcare workforce rather than buildings, continuity of healthcare operations, and the ability to provide healthcare in a flexible and adaptable manner;
- Have had the opportunity to begin to provide insights and guidance on the unique needs, concerns, and perspectives of their organizations or members;

- Will maintain partnerships for CI/KR protection with appropriate Federal, State, regional, local, tribal, and international entities; other private-sector entities; and nongovernmental organizations;
- Will work with the Department of Homeland Security and the Department of Health and Human Services to find suitable mechanisms to share CI/KR protection-related information; and
- Understand that their participation creates no legally binding agreements or liabilities.

Jim Bentley
Healthcare SCC Co-Chair

Hal S. Muller
Healthcare SCC Co-Chair

Table of Contents

List of Figures

List of Tables

Executive Summary

The Healthcare and Public Health Sector-Specific Plan (SSP) was created to complement the National Infrastructure Protection Plan (NIPP) by developing efforts to improve the protection of the sector in an all-hazards environment. The Healthcare and Public Health SSP establishes a relationship between government and the private sector to foster the cooperation necessary to improve the protection of the sector from a natural or manmade disaster. The plan sets a path forward for the sector to collectively identify and prioritize its assets, assess risk, implement protective programs, and measure the effectiveness of its protective programs. This document reflects the collaborative efforts between government stakeholders and public and private sector members who are dedicated to the protection of key resources within the Healthcare and Public Health Sector.

The Department of Health and Human Services (HHS), in its role as Sector-Specific Agency (SSA), and in collaboration with government and private sector security partners, developed this SSP. The sector is highly diverse in its composition and relationships with its many systems, networks, services, facilities, functions, and roles, both public and private, needed to prevent disease and disability, treat patients, foster public health, and respond to incidents requiring medical and public health services. The private sector, as well as various Federal, State, and local agencies, provide healthcare and public health services and participate in ongoing surveillance and detection of potentially devastating threats to the Nation's critical infrastructure and key resources (CI/KR) from terrorism and other manmade and natural threats. If these threats were realized, the result could seriously impact public health and economic vitality. In addition, many other sectors rely on Healthcare and Public Health Sector assets and services to ensure resiliency in the face of threats that may result in serious public health consequences (e.g., pandemic influenza).

The SSP is divided into eight sections based on guidance promulgated by the Department of Homeland Security (DHS) to ensure some consistency across all sectors. A brief summary of each section follows.

1. Sector Profile and Goals

Section 1 of the SSP provides an overview of the Healthcare and Public Health Sector, which consists of a full array of acute hospital and ambulatory healthcare, public health, mental health, substance abuse treatment, environmental and occupational health, long-term care, tele-health, pharmaceuticals, public health information, mortuary services, medical supplies, and other goods and services. In public health and medical emergencies, additional capabilities, such as mass vaccination; mass casualty and mortality services; and medical surge for additional numbers of ill, injured, or worried citizens, must be efficiently coordinated within the sector to ensure resiliency across other CI/KR sectors.

The section also briefly describes the entities that play a role in helping to secure the sector, including all levels of government and the private sector. These entities are referred to as "security partners." In the Healthcare and Public Health Sector, the primary Federal security partners include the DHS, the Department of Defense (DoD), and the Department of Veterans

Affairs (VA). These departments, along with other Federal agencies and State, local, and tribal governments, are represented on the Healthcare and Public Health Government Coordinating Council (GCC), which is chaired by HHS. Many members of the private sector also are critical to sector security and have formed the Healthcare Sector Coordinating Council (SCC). Together, the GCC and SCC represent a partnership between government and sector owners and operators to address CI/KR protection within the sector.

This section also describes the sector's vision and goals, which include the following:

Sector Vision: The sector will achieve overall resiliency against all threats, both natural and manmade. It will prevent or minimize damage to, or destruction of, the Nation's healthcare and public health infrastructure. It will preserve its ability to mount timely and effective responses to both routine and emergency situations. It will protect its critical workforce from harm resulting from terrorist or criminal activities, from natural disasters, and from serious infectious disease outbreaks, including those originating outside the United States.

Sector Goals: Derived from the vision statement are the following three categories of sector goals supported by high-level objectives: (1) workforce security, which includes protecting against threats, both natural and manmade, that have the ability to harm the sector's workforce; (2) physical security; and (3) cyber security.

Finally, the section briefly addresses the value proposition for undertaking this effort.

2. Identify Assets, Systems, Networks, and Functions

Section 2 of the SSP discusses ongoing efforts by government agencies and sector security partners to identify the sector infrastructure—assets, systems, networks, and functions—that could, if compromised, result in serious national economic or public health impacts.

In order to effectively manage sector efforts using a risk-based approach, HHS first needs to identify what critical infrastructures make up the sector. HHS and sector security partners have developed a taxonomy to categorize the sector. In addition, HHS, in conjunction with DHS, identified candidate assets that were recorded in the National Asset Database, along with assets collected from various other sources.

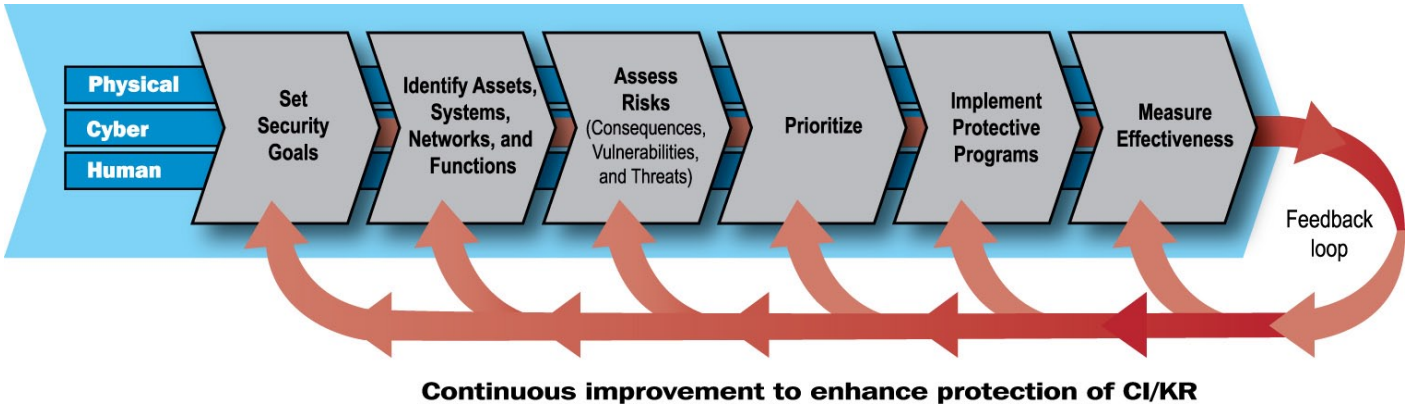
Looking forward, this section lays out plans for working with sector security partners to revisit the current methodologies. In doing so, it addresses issues associated with: (1) identifying appropriate information elements (e.g., what information is needed to conduct risk-based analyses), (2) issues associated with collecting data (e.g., where is information already available and what are the barriers to sharing information with private sector security partners), (3) issues associated with verifying data and keeping it up to date, and (4) issues associated with the security of sector data.

3. Assess Risks

The NIPP risk management framework (see the following figure) establishes the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national, sector, and individual asset, system, or network risk.

Central to that framework is the assessment of the three factors used to calculate risk—consequence, vulnerability, and threat. Sector security partners (governmental, private sector, and international) undertake CI/KR protection-related assessments under numerous mandates and market imperatives. Considering the wide variety of manufacturing, storage, and distribution facilities in the sector, these security assessments are site- and activity-specific. In order for the results of these risk assessments to be useful, not only for the development of individual security programs, but also for the informed allocation of resources, the results of these assessments must be comparable, both within the sector and across all CI/KR sectors.

Figure ES-1: NIPP Risk Management Framework



Working with the DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and Risk Management Division (RMD), HHS is working toward a tailored risk-management framework consistent with NIPP guidance. Earlier efforts have identified numerous tools and methodologies applicable within the sector. HHS continues to examine practices within and across sectors to determine best-fit risk management processes, quantify the interdependencies between the Healthcare and Public Health Sector and its other security partners, identify gaps in CI/KR protection, and develop protective programs to close or mitigate these gaps.

Before performing detailed assessments, it is prudent to prescreen the candidates identified through previous assessment. To date, HHS has used two screening methodologies; one scenario-based and one based on identifying critical functions, to identify candidate CI/KR and their supporting workforce. Only those candidates with significant potential consequences are then asked to perform a detailed consequence analysis and vulnerability assessment. Moving forward, HHS will work with its security partners to revisit the topics of refining criteria for screening assets and best-practice methodologies for conducting risk, consequence, and vulnerability assessments.

Finally, it is important to note that the ability to conduct accurate and timely threat assessments is not normally within the purview of many private sector security partners. Most, therefore, rely on HHS and DHS to provide useful threat information. HHS will continue to work with DHS to ensure efficient sharing of threat information among all of our security partners.

4. Prioritize Infrastructure

The NIPP requires that the National CI/KR Protection Program prioritize efforts across sectors so that public resources are applied where they offer the most benefit for reducing risk. In a similar manner, the Healthcare and Public Health Sector must prioritize assets and protective actions to maximize the use of sector resources while keeping information useful as input to the national effort.

HHS has participated in prioritization efforts sponsored by DHS, and as we move forward, this process will continue with the consultation of representatives of DHS, VA, DoD, the GCC, and the SCC. Prioritization is an iterative process. Its long-term success depends on flexible readjustments in the light of experience, success in developing protective programs, changes in the threats faced, and other factors.

5. Sector Protective Programs

Like other SSAs, HHS is not solely responsible for the development and implementation of protective programs across the sector. It does, however, facilitate the effective implementation of protective programs by coordinating with its public, private, and other security partners. The overall intent of protective programs is to manage risk by deterring threats, mitigating vulnerabilities, and/or minimizing consequences. The most effective protective programs are comprehensive, coordinated, cost-effective, risk-based, consistent with established programs, and sensitive to the cultural differences that may exist among the affected parties.

Many programs have been initiated and/or continued across the sector during the past year. Some have been the result of Homeland Security Presidential Directive-7 (HSPD-7) requirements; others have been brought about by legislation or general awareness of additional threats facing the sector in the post-9/11 environment.

The sector's protective programs target physical, cyber, and workforce CI/KR elements. Across the sector, some programs are well developed, while others are not. At the Federal level, all Cabinet-level departments with healthcare and public health responsibilities have a range of protective programs in place. All are required by legislation; some are unique to each department, some are applicable across all public agencies, and a few are applicable to all elements of the sector.

In addition, the private sector has a wide variety of protective programs in place or under development. In addition to those mandated by Federal, State, or local authorities, private sector programs have been developed in response to accreditation or regulatory requirements and/or market pressures of various kinds.

This section of the SSP describes the major protective programs in the sector that target physical, cyber, and/or workforce elements. Among other things, this description shows the variety of organizations and mandates involved. This, in turn, indicates that no single program is appropriate to address all sector needs; however, a combination of tailored programs can provide the needed protection. This section also discusses sector plans to coordinate efforts more closely and share best practices as plans move forward.

6. Measure Progress

Appropriate metrics must be employed to measure progress made toward CI/KR protection goals. These metrics, in turn, provide feedback leading to improved resource allocation. DHS develops national-level core metrics that are designed to apply to all CI/KR and enable comparison and analysis of progress made in each sector. In addition, each sector develops sector-specific metrics that focus on the unique CI/KR protection-related characteristics of that sector. Three kinds of metrics are under development in the sector—descriptive, process, and outcome metrics. This section discusses the broad metrics the sector is considering and outlines how HHS will work with DHS and its security partners to continue to refine metrics to ensure that appropriate measurement and feedback mechanisms exist within the sector.

7. Planning Healthcare and Public Health Research and Development

This sector, like all others, relies on new technologies to assist in the protection of major assets. These technologies can help preserve and strengthen the sector's ability to meet the Nation's CI/KR protection needs. Major research and development (R&D) goals of interest to the sector have been previously identified, and many R&D projects conducted across the Federal Government have undergone preliminary review for their applicability to sector needs.

This section gives an overview of current efforts in place, outlines sector goals for R&D, and maps these goals to the central themes discussed in the National Plan for Research and Development in Support of Critical Infrastructure Protection, promulgated by the White House Office of Science and Technology Policy (OSTP). This section also describes some of the sector R&D requirements and discusses sector plans to develop an R&D plan specific to the Healthcare and Public Health Sector.

8. Managing and Coordinating SSA Responsibilities

The HHS Office of the Assistant Secretary of Preparedness and Response (ASPR – formerly known as the Office of Public Health Emergency Preparedness (OPHEP)) manages sector SSP development on behalf of its sector partners. During the development and implementation of the SSP, HHS will work closely with security partners at various levels, including Federal, State, local, and tribal governments, and the private sector. As described above, coordination on the government side will occur through the GCC; on the private sector side, the coordination will occur through the SCC. The SSP will be updated as the NIPP is updated. The SSP will also be updated as warranted by changes in the sector's security posture or processes, or by real-world events and exercises. To ensure accuracy and reinforce the partnership nature of this effort, the SCC and the GCC will participate in any update to the SSP.

Appendices

In addition to the information contained in the sections, additional useful information is presented in the appendices. A brief summary is provided as follows:

- Appendix 1 provides a list of acronyms and abbreviations;
- Appendix 2 contains a glossary of key terms;
- Appendix 3 reviews CI/KR protection applicable authorities within the sector;
- Appendix 4 summarizes risk and vulnerability tools and methods reviewed during the past year;
- Appendix 5 presents a sampling of protective programs in the sector; and
- Appendix 6 lists the member organizations of both the GCC and SCC.

Introduction

Protecting the critical infrastructure and key resources (CI/KR) of the United States is essential to the Nation's security, economic vitality, and way of life. CI/KR include the assets, systems, networks, and functions that provide vital services to the Nation. Terrorist attacks on CI/KR and other manmade or natural disasters could significantly disrupt the functioning of government and business alike. They can produce cascading effects far beyond the affected CI/KR sector and physical location of the incident. Direct attacks could result in large-scale human casualties, property destruction, and economic damage, and profoundly harm national prestige, morale, and confidence. Terrorist attacks that use components of the Nation's CI/KR as weapons of mass destruction (WMDs) could have even more devastating physical, psychological, and economic consequences.

Protection Needed

The protection of CI/KR is, therefore, an essential component of the homeland security mission to make America safer, more secure, and more resilient from terrorist attacks and other natural and manmade hazards. Protection includes actions to guard or shield CI/KR assets, systems, networks, or their interconnecting links from exposure, injury, destruction, incapacitation, or exploitation. This includes actions to deter, mitigate, or neutralize the threat, vulnerability, or consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, including hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting personal surety programs, and implementing cyber security measures.

National Planning Framework

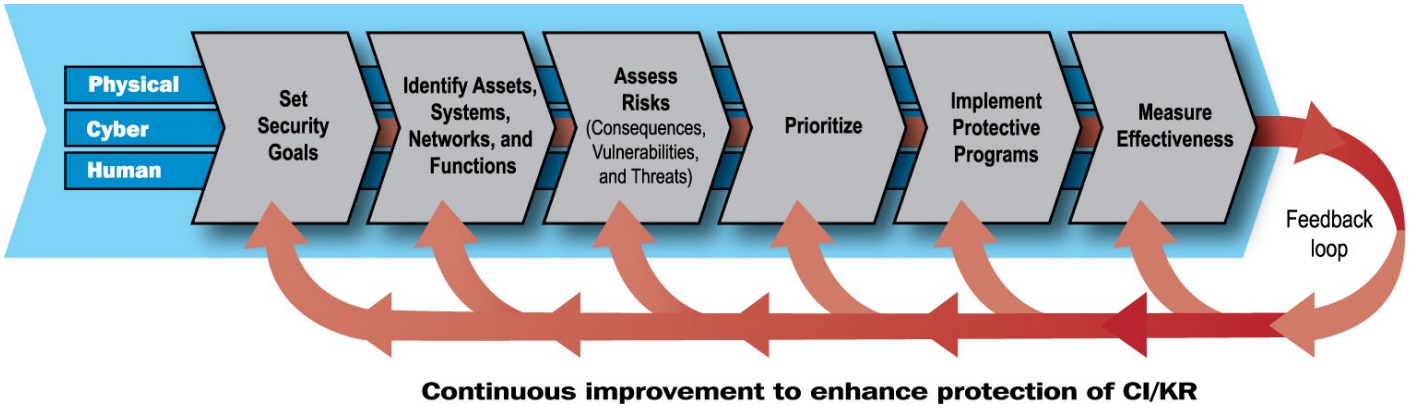
The National Infrastructure Protection Plan (NIPP) provides the framework for the unprecedented cooperation needed to develop, implement, and maintain a coordinated national effort that strengthens government at all levels, the private sector, and international organizations and allies. The NIPP provides a consistent, unifying structure for integrating both existing and future CI/KR protection efforts. It also provides the core processes and mechanisms to enable government and private sector security partners to work together to implement CI/KR protection initiatives. Homeland Security Presidential Directive 7 (HSPD-7) outlines 17 CI/KR sectors and recognizes that each sector possesses unique characteristics and operating methods.

Sector-Specific Plans

The purpose of the Sector-Specific Plans (SSPs) is to detail the application of the NIPP risk management framework to each of these 17 CI/KR sectors. SSPs are developed by the designated Federal Sector-Specific Agencies (SSAs) in coordination with relevant sector security partners. The SSP for each sector aligns with the processes established in the NIPP, most notably the risk management framework. Each SSP supports the planning assumptions outlined in the NIPP, as well as sector-specific planning assumptions that are relevant to protection of that sector's CI/KR.

This document presents the SSP for the Healthcare and Public Health Sector.

Figure I-1: NIPP Risk Management Framework



The NIPP risk management framework, the cornerstone of the NIPP, includes the following activities:

- Set security goals that define specific outcomes, conditions, end points, or performance targets that collectively constitute an effective protective posture;
- Identify critical infrastructures, including assets, systems, and networks both inside the United States and elsewhere, the critical functionality they provide, and pertinent information on them relevant to risk management;
- Assess risks by combining potential direct and indirect consequences of a terrorist attack or other hazard, known vulnerabilities to various potential attack vectors, and general or specific threat information;
- Prioritize asset, system, and network criticality in order to establish protection priorities and provide the basis for protection planning and the informed allocation of resources;
- Implement protective programs to reduce the risks identified and to secure the resources needed to address priorities; and
- Measure the effectiveness of protective programs at the national and sector levels to measure progress and to assess the effectiveness of the national CI/KR protection.

1. Sector Profile and Goals

The 2006 Healthcare and Public Health SSP for CI/KR protection has been prepared to meet an annual requirement established by HSPD-7. HSPD-7 requires the development of a sector-wide plan to protect CI/KR identified by the sector. Sector CI/KR have been identified based on how they are defined under the Homeland Security Act of 2002 as follows:

- Critical infrastructure means "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters"; and
- Key resources are defined as "publicly or privately controlled resources essential to the minimal operations of the economy and government."[1]

Critical infrastructure protection includes all activities directed at safeguarding people, systems, and physical infrastructure that are indispensable to the operations of critical infrastructure sectors and their ability to provide essential goods and services.

This SSP is directed toward everyone involved in healthcare and public health: managers, owners, and operators of the sector's assets, systems, networks, and functions; public health planners; grant providers; emergency managers at all levels; and it includes their respective workforce. The Healthcare and Public Health SSP for 2006 lays the groundwork for a comprehensive, actionable strategy to improve protection efforts nationally. This SSP will be added as an annex to the NIPP issued by the Department of Homeland Security (DHS) and integrated into a broader framework for protection efforts across all 17 sectors.

The NIPP focuses on threats facing sector CI/KR across all hazards—natural, manmade, and acts of terrorism—prioritizing protection efforts in a unified structure provided by a single national protection plan. This SSP addresses the sector's approach to protecting identified CI/KR and is not a response plan. With the goal of sector resiliency, the SSP emphasizes identifying, prioritizing, protecting, and sustaining the sector's CI/KR. While the SSP reflects a separate and distinct framework for protection of CI/KR, the National Response Plan (NRP) contains the national strategy for response and recovery. Within the NRP, the Department of Health and Human Services (HHS) is assigned as the responsible agency for Emergency Support Function 8 (ESF-8), which encompasses all public health and medical response. DHS is leading a national effort to clarify the relationship between the NIPP and the NRP, and it is expected that a CI/KR Protection Support Annex to the NRP will be incorporated in the next NRP update in 2007.

Major topics in this section include the following:

- Sector profile;

[1] See Homeland Security Act of 2002, Public Law 107-296, Section 2, Definitions. c Law 107-296, Section 2, Definitions.

- Security partners;
- Sector security goals;
- Value proposition; and
- The path forward.

1.1 Sector Profile

The Healthcare and Public Health Sector constitutes approximately 15 percent of the Gross National Product (GNP),[2] equal to $1.86 trillion, and has an important impact on the U.S. economy. Privately owned and operated organizations comprise approximately 90 percent of the sector and identify themselves with the delivery of healthcare goods and services. The public health component is composed largely of government agencies at the Federal, State, local, and tribal community levels. The public health component is not as large as the private component and performs a somewhat different array of functions, concentrating largely on preventive measures. The sector is highly diverse in its composition and relationships with its many systems, networks, services, facilities, functions, and roles, both public and private, needed to prevent disease and disability, treat patients, foster public health, and respond to incidents requiring medical and public health services.

The sector provides a full array of goods and services for acute hospital and ambulatory healthcare, public health, public health information, mental health, substance abuse treatment, environmental and occupational health, long-term care, tele-health, pharmaceuticals, mortuary services, medical supplies, and others. Private sector as well as Federal, State, and local agencies provide healthcare and public health services, and participate in ongoing surveillance and detection of potentially devastating threats to the Nation's CI/KR from bioterrorism and other manmade and natural threats.[3] In public health and medical emergencies, additional capabilities such as mass vaccination, mass casualty and mortality services, and medical surge involving additional numbers of ill, injured, or worried citizens must be efficiently coordinated within the sector to permit essential healthcare for the Nation.

The sector's diverse workforce is essential to the continuity of sector functions and is dependent on many other sectors. The sector workforce can be found in medical treatment facilities; public health agencies; State and local centers for the aging; nursing homes; rehabilitation centers; group homes; academic institutions; healthcare clearinghouses; healthcare information technology and systems activities; pharmacies; laboratories; food processing, handling, and distribution centers; decontamination facilities and services; and fatality services. The workforce includes healthcare personnel, clinical providers, biomedical engineers, pharmacists, occupational health providers, medical materiel suppliers, transplant and blood product providers, health insurance and other third-party payers, mortality services workers, and many others.

Elements of the sector are present in virtually all U.S. communities, although at varying levels of capability. Although the sector does have several major, nationally organized entities, the sector is highly decentralized.[4] Composed of both private and governmental entities, the boundaries between the two are often indistinguishable.

Table 1-1 provides an overview that gives a sense of the size and breadth of the sector. It includes private sector and government data for comparison.

[2] According to U.S. National Economic Accounts, the U.S. Gross Domestic Product was $12.456 trillion in 2005. The Healthcare and Public Health Sector was estimated to be approximately 15 percent of that total or $1.868 trillion.

[3] This definition includes suggestions by the SCC reviewers during September 2006.

[4] Examples of organizations that are national in scope include the Hospital Corporation of America, Tenet Healthcare Corporation, and the Veterans Health Administration. In addition, some sector elements are required to function and operate independently, based on Federal safe harbor and anti-trust laws. These examples were suggested by SCC reviewers during September 2006.

Table 1-1: Summary of the Healthcare and Public Health Sector

Major Element	Private Sector	Public Sector			
		Federal	State	Local	Tribal
Healthcare personnel	> 13,000,000[5]	> 450,000[6]			
Hospitals (including specialty hospitals)	5,525[7]	~ 350[8]	1,121		36
Ambulatory facilities (including office practices and dental offices)	300,000	~ 490,000 (unable to separate by ownership; some may be private)[9]			
Long-term care facilities	~ 70,000 (unable to separate by ownership)[10]				
Home health agencies	6,928 (unable to separate by ownership)[11]				
Pharmacies	~ 70,000[12]				
Health departments		Parts of HHS, the Environmental Protection Agency, Department of Defense, and Department of Veterans Affairs	57	~3,000	36
Health-related laboratories	~ 2,000 (unable to separate by ownership)				
Health-related laboratories	~ 172,000[13]	~ 2,000 (unable to separate by ownership)[14]			
Pharmaceutical manufacturers	> 2,500[15]				

[5] Falling within this broad category are many professional categories. Included are approximately 5 million first-responders with at least some emergency medical training, approximately 3 million registered nurses, and more than 800,000 physicians. In alphabetical order, the overall figure includes, but is not necessarily limited to, the following: ambulance drivers and attendants; behavioral health professionals; clinical laboratory technologists and technicians; emergency management specialists; emergency medical technicians and paramedics; firefighting occupations with medical capabilities; hazardous materials removal workers; nuclear medicine technologists; nurses; occupational health and safety specialists; pharmacists; physicians; physician assistants; radiological technologists and technicians; respiratory therapists; veterinarians; and volunteer firefighters with medical capabilities. See Department of Health and Human Services (HHS), Health Resources and Services Administration. Preliminary findings for the 2004 national sample survey of registered nurses, http://bhpr.hrsa.gov/healthworkforce/reports/rnpopulation/preliminaryfindings.htm. See HHS, Health Resources and Services Administration, 2006. Physician supply and demand, projections to 2020, HRSA-230-BHPr-27(2), http://bhpr.hrsa.gov/healthworkforce/reports/physiciansupplydemand/currentphysicianworkforce.htm.

[6] See HHS, Health Resources and Services Administration, The Public Health Workforce Enumeration, 2000, HRSA/ATPM Cooperative Agreement # U76AH00001-03, ftp://ftp.hrsa.gov//bhpr/nationalcenter/phworkforce2000.pdf.

[7] See American Hospital Association, www.ahadata.com.

[8] See Kaiser Commission on Medicaid and the Uninsured, *Stresses to the Safety Net: The Public Hospital Perspective,* June 2005. Also see National Association of Public Hospitals and Health Systems, www.naph.org; and www.defenselink.mil, www.airforcemedicine.afms.mil, http://home.pcisys.net/~pwebber/milhosp1.htm, www.cnrc.navy.mil/richmond/naval_medical_facilities.htm, www.vha.gov.

[9] See U.S. Census Bureau, 2003 Economic Census, Table 1: Advance Summary Statistics for the United States, 2002, NAICS Basis, www.census.gov/econ/census02/advance/TABLE1.htm; and U.S. Census Bureau, Ambulatory Health Care Services, 2002, Document ECO2-621-01, www.census.gov/econ/census02/guide/INDRPT62.HTM.

[10] The are many subcategories of such facilities, including group homes for the disabled with nursing care, homes for the aged with nursing care, homes for the elderly with nursing care, hospices, nursing care facilities, nursing homes, rest homes with nursing care, retirement homes with nursing care, and skilled nursing facilities. See U.S. Census Bureau, 2002, NAICS Definitions, 623 Nursing and Residential Care Facilities, www.census.gov/epcd/naics02/def.

[11] This category of facilities includes centers devoted to hospice care, hospital care, pharmacy services, physicians, practice administration, rural health, and skilled nursing. See HHS, Centers for Medicare and Medicaid Services, www.cms.hhs.gov/center/hha.usp.

[12] See National Council for Prescription Drug Programs, www.ncpdp.org.

[13] Approximately 90,000 are located in physicians' offices. See Online Survey and Certification Reporting System (OSCAR) database, Centers for Medicare and Medicaid Services, Baltimore, Maryland. See also General Accounting Office, 1999, *Emerging Infectious Diseases: Consensus on Needed Laboratory Capacity Could Strengthen Surveillance,* Report to the Chairman, U.S. Senate Subcommittee on Public Health; Committee on Health, Education, Labor, and Pensions, February, Document No. GAO/HEHS-99-26, available at www.gao.gov.

[14] Of particular interest are laboratories that are part of the Laboratory Response Network, including national laboratories, reference laboratories, and sentinel laboratories. Data drawn from the Online Survey and Certification Reporting System (OSCAR) database, Centers for Medicare and Medicaid Services, Baltimore, Maryland.

[15] See Pharmaceutical Manufacturer Information, www.drugs.com/manufacturers.

Major Element	Private Sector	Public Sector			
		Federal	State	Local	Tribal
Medical device and supply companies	> 1,000[16]				
Blood products centers	> 500[17]	2			
Health insurers and other payers	1,300[18]	1	50		

1.1.1 Public-Private Interaction

The Healthcare and Public Health Sector entities work together daily to manage supplies, provide clinical care, manage patients, manage payment processes, order pharmaceuticals, work with mortuary services, and respond to major disasters or terrorist attacks. These entities are also interconnected by networks that disseminate clinical and public health information. Some healthcare facilities operate as free-standing entities, but most are part of a local or regional network, whether formalized or not, that share patients through referrals, services, and professional staff. Except during catastrophic events, healthcare and public health tend to be organized and carried out locally.

1.1.2 Significant Gaps and Overlaps

The Healthcare and Public Health Sector overlaps with functions of other sectors identified in HSPD-7. These functions include State and Territorial emergency management offices possessing some medical response capabilities, and local emergency response units of various kinds, some containing medically trained personnel.[19] A second sector overlap involves law enforcement bodies within the Emergency Services Sector that would be needed for security in health emergencies and for implementation of such countermeasures as area quarantine and mass vaccinations.[20] A third overlap involves the 40,000 commercial pharmacies in the country that are a part of the Commercial Facilities Sector.[21] Recognizing these overlaps, HHS continues to work closely with DHS to assure a unified approach to CI/KR protection issues involving such cross-sector dependencies.

1.1.3 Significant Interdependencies

Sector organizations at the Federal, State, and local levels interact with each other and with public safety organizations, emergency response agencies, private enterprises, and volunteer organizations at all levels of society. More specifically, the sector depends on several other sectors in significant ways as shown in table 1-2.

Table 1-2: Sector Interdependencies

Interdependent Sector	Interdependency
Transportation Systems	Movement of supplies, raw materials, pharmaceuticals, personnel, emergency response units, patients, and fatalities.
Communications	Third-party reimbursements and other business processes.

16 See HHS, Centers for Medicare and Medicaid, *Health Industry Market Update: Medical Devices and Supplies*, December 2004.

17 See American Association of Blood Banks Locator Database, www.aabb.org/Locator/Locator.asp.

18 See America's Health Insurance Plans Association, www.ahip.org.

19 Under HSPD-7, paragraph 15, these fall within the emergency services sector for which DHS is the SSA.

20 Under HSPD-7, paragraph 15, these fall within the emergency services sector for which DHS is the SSA.

21 Under HSPD-7, paragraph 15, these fall within the commercial facilites sector for which DHS is the SSA.

Interdependent Sector	Interdependency
Energy	Electric, natural gas, propane, and diesel fuel to power and run facility functions of all kinds, including facility protection programs.
Water	Healthcare, pharmaceutical operations, and sanitization services.
Emergency Services	Coordination with first-responders and Emergency Medical Services, and includes local law enforcement for security for various emergencies (e.g., quarantine, imposed isolation, etc.).
Information Technology	Business, clinical, and security information systems.
Postal and Shipping	Movement of equipment and supplies.
Chemicals	Support to the pharmaceutical industry.
Food and Agriculture	Food production and distribution for healthcare and public health personnel and patients.
Local Law Enforcement	Security for various emergencies, such as quarantine and imposed isolation.

All other sectors in the U.S. economy are dependent upon the Healthcare and Public Health Sector in disasters and non-disaster situations to achieve, restore, and maintain human health.

1.1.4 Authorities Governing the Sector

All entities in the sector are subject to a wide range of legislative and regulatory authorities (see appendix 3). These authorities and constraints exist at the Federal, State, and local levels.

1.1.5 Workforce Threats Facing the Sector

The sector's healthcare and public health workforce of over 13 million personnel is its most important asset. While facilities, systems, and equipment are important and not mutually exclusive, the professional workforce of Federal, State, local, and tribal public health agencies and private sector hospitals and other healthcare organizations provides critically important health goods and services upon which the Nation, as a whole, depends.

Two principal types of threats to the Healthcare Sector's workforce have been identified to date—an attack by terrorists or criminals against the sector's workforce, and all non-terrorist events such as weather-related threats, earthquakes, and disease epidemics that threaten workers in all workplaces settings.

1.1.6 Physical Threats Facing the Sector

The Healthcare Sector has comparatively few individual high-value facilities likely to be targeted by terrorists for physical attacks. Although threat intelligence reveals that attacks on ambulances and hospitals in foreign countries have occurred, none have been suspected domestically to date. However, the vulnerability of healthcare facilities must be considered because they are inherently susceptible to attack based on their public accessibility. The predisposition of facilities to structural damage during natural disasters remains a concern. Minimizing the physical vulnerabilities of its CI/KR is a major objective of the sector.

1.1.7 Cyber Threats Facing the Sector

The Healthcare Sector is increasingly electronically interconnected. This trend is spurred by market forces; increasing information technology (IT) capabilities; the growing promise of IT in improving sector efficiency and effectiveness; the use of telemedicine to provide rural healthcare support; and multiple Federal, State, local, and private sector initiatives such as regional health information organizations. Accompanying these advancements are potential IT vulnerabilities much like those facing other sectors.

1.1.8 Mass Casualty Threats Facing the Sector

The sector is also susceptible to catastrophic events creating mass casualties (e.g., pandemic influenza). Such events can overwhelm the surge capacity of healthcare and public health facilities and services with the influx of patients. Catastrophic events can also reduce the number of healthcare providers available to treat existing patients. Given the importance of the uninterrupted provision of care during such events, and the relationship in all sectors between a healthy workforce, and sector resilience and continuity of operations, the effects of such events on the healthcare system are considered of significant importance to the sector.

1.2 Sector Partners

Sector partners/collaborators that participate in the NIPP planning process include Federal agencies; interagency groups; public and private advisory councils; academic research centers; thinks tanks; State, Territorial, local, and tribal governments; regional bodies; international partners; and private sector owners, operators, and their various suppliers.[22]

1.2.1 Private Sector Owners and Operators

Immediately following HSPD-7 promulgation, HHS promoted the involvement of private sector entities in CI/KR protection as partners in the formation of the Sector Coordinating Council (SCC). By 2006, this involvement comprised more than nine sub-councils or interest areas identified in Section 8 of this SSP. These private partners make essential contributions to the SSP, as well as to sector preparedness and response capabilities.

The timely sharing of information in coordination with private sector partners bears on the overall sector safety and security. The private sector's willingness to share situational awareness information during the response to Hurricane Katrina is just one example of how information sharing and coordination has been leveraged through the partnership between HHS and its private sector security partners.

1.2.2 Major Federal Agencies

Healthcare and public health responsibilities are shared among five Cabinet-level departments. These include the Departments of Health and Human Services, Veterans Affairs, and Defense, all of which have direct healthcare and public health programs. DHS is responsible for the overall national coordination of CI/KR protection as detailed in HSPD-7, and for providing major emergency response capabilities such as that of the Federal Emergency Management Agency (FEMA) and the U.S. Coast Guard. The Department of Labor's (DOL's) Occupational Safety and Health Administration (OSHA) also works to protect the American workforce from job-related hazards.

1.2.3 Selected Federal Interagency Groups Oriented Toward Security Issues

HHS security personnel serve on three major interagency groups: the Interagency Security Committee, focusing on all aspects of physical security; the Information Sharing Council; and the National Cyber Response Coordination Group, addressing cyber

[22] The term "partner" should be interpreted in its collaborative sense. No legal partnership is implied by the term.

security issues. HHS participation in these and other security forums provides a means to highlight the sector's CI/KR protection and emergency preparedness issues.

1.2.4 Advisory Councils

HHS has worked with advisory councils on many health-related topics to date. During the upcoming year, HHS will continue to work with advisory councils devoted to CI/KR protection-related topics (e.g., physical, cyber, and workforce security issues) in consultation with the sector's Government Coordinating Council (GCC) and SCC established pursuant to the NIPP.

1.2.5 State, Territorial, Local, and Tribal Governments

State, Territorial, local, and tribal governments are responsible for identifying and protecting CI/KR within their respective jurisdictions. HHS has collaborated with three major associations for years on health matters and more recently as integral members of the sector GCC. These major associations are the Association of State and Territorial Health Officials (ASTHO), the National Association of County and City Health Officials (NACCHO), and the Association of Public Health Laboratories. These bodies represent State and local public health officials and agencies, and State, county, and city public health laboratories, respectively.[23] This partnership has broadened to include CI/KR protection.

HHS continues to work to draw tribal health representatives into CI/KR protection planning discussions and to encourage tribal representation on the GCC. This participation is necessary because tribal areas may also be vulnerable to natural disasters and to terrorist attacks. Their connection with outside support agencies or associations in the event of a disaster is essential, and HHS will continue to strengthen its collaboration with tribal entities in the coming year.

1.2.6 Academia, Research Centers, and Think Tanks

HHS continues to establish formal relationships with academia, research centers, and think tanks to promote the development of methodologies, technology research, and training in CI/KR protection-related issues. The Healthcare and Public Health Sector acknowledges the importance of their contribution and will continue to forge these linkages in the coming year as the sector's critical asset identification and protective programs and measures are matured. The value of established, as well as experimental, methodologies, assessments, and metrics appropriate to healthcare cannot be underestimated in terms of the sector's continued evolution. The Healthcare and Public Health Sector will pursue these methodologies, assessments, and metrics in the coming year in consultation with the Department of Defense (DoD), the Department of Veterans Affairs (VA), and relevant private sector partners.

1.2.7 International Organizations and Foreign Countries

HHS continues its relationship with the Secretariat of the World Health Organization (WHO) and other partners, to include those leading U.S. Government efforts in the surveillance and detection of disease outbreaks overseas. The Office of the Assistant Secretary for Preparedness and Response (ASPR), in coordination with the HHS Office of Global Health Affairs, is continually working on global activities related to pandemic influenza preparedness and response to include strengthening the pandemic influenza preparedness and response capacity of Cambodia, China, Indonesia, Laos, and Vietnam through prevention and containment, and screening visa applicants residing outside the United States for infectious diseases prior to entering the United States. Within HHS ASPR, the Office of Science, Medicine, and Public Health is the key link to the international community for public health readiness efforts.

[23] Another example is HHS's coordination with the AABB Inter-Organizational Task Force on Domestic Disasters and Acts of Terrorism.

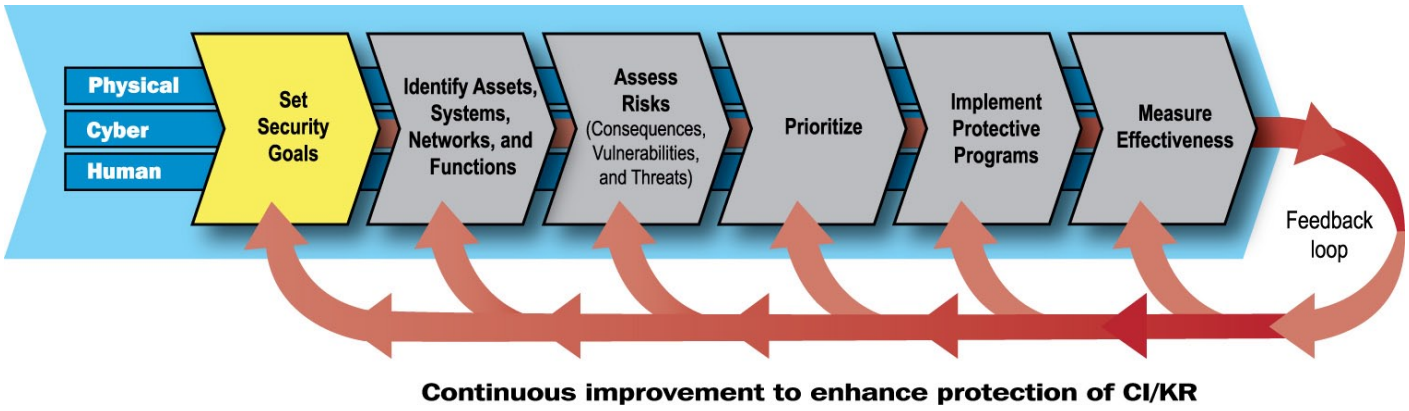
HHS international outreach is coordinated through several Federal departments and agencies (e.g., Department of State, Federal Bureau of Investigation (FBI), DoD, DHS), and others, as appropriate. In addition to the full range of safety and security topics, HHS assesses the existence and nature of relationships with, and reliance on, various levels of foreign governmental support; local and national organizations; and relationships with health, law enforcement, and security/intelligence ministries.

The sector has important shared infrastructures with Canada and Mexico, with many suppliers of pharmaceuticals and medical supplies maintaining facilities in other countries and Territories. Natural or manmade threats could interrupt the supply chains of healthcare products, affecting the delivery of goods and potentially resulting in adverse economic impacts. Acknowledging our mutual vulnerabilities, the Security and Prosperity Partnership framework was established in 2005. This trilateral effort aims to increase security and enhance prosperity among the United States, Canada, and Mexico through great cooperation and information sharing.[24] Critical infrastructure protection is an important part of this partnership, as is our influenza pandemic planning with these neighboring countries.

1.3 Sector Security Goals

The Healthcare and Public Health Sector adopted a vision statement and specific goals for the sector during 2006 that are consistent with the overall risk management program developed by DHS. Figure 1-1 summarizes the elements in this program.

Figure 1-1: Setting Security Goals



The sector's vision statement and goals are summarized below.

1.3.1 Vision Statement

The Healthcare and Public Health Sector will achieve overall resiliency against all threats—natural and manmade. It will prevent or minimize damage to, or destruction of, the Nation's healthcare and public health infrastructure. It will preserve its ability to mount timely and effective responses to both routine and emergency situations. It strives to protect its critical workforce from harm resulting from terrorist or criminal activities, from natural disasters, and from serious infectious disease outbreaks, including those originating outside the United States.

[24] For further information, see www.spp.gov.

1.3.2 Long-Term Workforce Security Goals

Three long-term workforce security goals have been identified for the sector. The first is to deny terrorists the ability to exploit those critical services that enable the healthcare and public health workforce to carry out their mission, including support services such as food and water supply, medications, fire prevention, and radiological detection. The second is to deny terrorists and insiders the ability to exploit the provision of services that are afforded through the healthcare and public health workforce, including, but not limited to, such critical services as health surveillance, disease detection, protection against pathogens, community health interventions (e.g., quarantine, mass vaccination, and delivery of antivirals), and direct attacks on workforce members while en route to, or in the process of, providing patient care.[25] The third is to protect workforce members from the unintended consequences of natural and manmade disasters, such as hurricanes, flooding, fire, bio-contagious disease, biological hazards, chemical hazards, etc.

1.3.3 Long-Term Physical Security Goals

Three long-term physical security goals have been identified for the sector. The first is to prevent external attacks by terrorists, criminals, and others using weapons either easily produced or locally available (e.g., small arms, conventional explosives, suicide bombers, chemical or biological weapons). The second is defending against potential attacks or disruption of services by insiders capitalizing on their expert knowledge of structural vulnerabilities and other physical security weaknesses. The third is protecting the physical structure from the unintended consequences of natural or manmade disasters, such as hurricanes, flooding, fire, electrical storms, and other severe weather occurrences.

1.3.4 Long-Term Cyber Security Goals

Three long-term cyber security goals have been adopted by the sector. The first is to prevent unauthorized use of, or exploitation of, electronic information and communications systems by terrorists, criminals, and others. The second is defending against potential internal cyber attacks intended to cause disruption or denial of services, attacks that are intended to gain access to sensitive data or data systems, and defending against other nefarious acts that pose a risk to the confidentiality, integrity and availability of healthcare information and the systems that store that information. The third is to protect against potential threats to cyber assets related to the unintended consequences of natural disasters, such as hurricanes, flooding, power outages, etc., in order to ensure continuity of healthcare operations.

Tables 1-3 through 1-5 provide the supporting objectives related to each of the long-term physical, cyber, and workforce security goals identified above.

1.3.5 Iterative Process to Establish Sector Security Goals

The process for establishing sector-wide security goals continues to take into account the complex nature of the sector (e.g., its complex, multilevel interrelationships; its "cottage industry" characteristics; its multiple regulatory compliance requirements; and its multiple missions). The process also addresses the roles that the sector's CI/KR play in mitigating and responding to terrorist threats, natural disasters, infectious disease outbreaks, and other threats.

Defining goals and aligning objectives is an iterative and dynamic process. This process includes evaluating the sector's security efforts, determining organizational interdependencies, interpreting communication flows, and evaluating historical data on response and planning during manmade or natural disasters. As a result, the goals will continue to be refined, added to, and reprioritized in consultation with the GCC, the SCC, and other security partners to ensure an achievable, sustainable sector security model.

[25] The sector is operating at a dangerously low level of staffing for almost all healthcare professions. The number of health professions instructors is also dropping and the force is aging. These factors create a situation in which the labor supply will continue to drop faster than new professionals can enter the workforce for the foreseeable future. These factors were pointed out by SCC reviewers in September 2006.

Table 1-3: Long-Term Workforce Security Goals and Supporting Objectives

Workforce Security Goals	Supporting Long-Term Objectives
Protection Against Terrorist Attacks	• Identify or ensure identification of facility physical vulnerabilities taking into account all physical structures (e.g., garages, parking lots, leased facilities) and access points; • Develop strategies for limiting access to facilities and their grounds that do not impede business processes associated with the day-to-day activities of professional staff, patients, and their visiting families, vendors, volunteers, contractors, suppliers, and others present in facilities on a regular or episodic basis; • Implement or ensure implementation of physical barriers and authentication mechanisms that limit access to facilities and their grounds; • Develop policies and procedures to enable the appropriate oversight of workforce members, volunteers, contractors, patients, vendors, and suppliers; • Develop, test, and conduct educational training and awareness programs to reduce the likelihood of threat to the physical security of facilities; and • Implement, test, and update Continuity of Operations Plan (COOP), taking into account response and recovery across multiple threat scenarios.
Protection Against Insider Attacks or Disruptions	• Identify facility vulnerabilities to insider threats or disruption; • Develop a strategy for validating the identity of all personnel, contractors, and volunteers; ensure that background checks on personnel have been completed, giving special consideration to those staff with access to sensitive systems, areas, or functions associated with facilities; • Implement practices for authenticating vendors, suppliers, and other external visitors to facilities outside of normal hours; and • Implement, test, and update COOP with a focus on physical security protection.
Protection Against Other Threats to Facility Staff	• Identify and prioritize vulnerabilities facing the facility's staff while at work; • Identify, validate, implement, and test mitigation strategies, including physical barriers to attacks that will protect the workforce; • Ensure that the appropriate strategies and technologies are in place for minimizing the risks facing the families of the workforce during large-scale crises as a means of reducing or eliminating the need for workforce members to choose between their professional responsibilities and their family's safety in such crises; • Ensure that adequate plans are in place to provide workforce members access to the worksite, including workforce food, shelter, and provisions for family members; • Design, test, conduct, and review training and awareness programs tailored to threats against the workforce on a regular basis; • Routinely test workforce security and make the results available to facility management for action, if required; and • Implement, test, and update COOP, taking into account response and recovery across multiple threat scenarios. COOPs must be tested and updated at appropriate intervals.

Table 1-4: Long-Term Physical Security Goals

Physical Security Goal	Supporting Long-Term Objectives
Protection Against Terrorist Attacks	• Identify or ensure identification of facility physical vulnerabilities taking into account all physical structures (e.g., garages, parking lots, leased facilities) and access points; • Develop strategies for limiting access to facilities and their grounds that do not impede business processes associated with the day-to-day activities of professional staff, patients, and their visiting families, vendors, volunteers, contractors, suppliers, and others present in facilities on a regular or episodic basis; • Implement or ensure implementation of physical barriers and authentication mechanisms that limit access to facilities and their grounds; • Develop policies and procedures to enable the appropriate oversight of workforce members, volunteers, contractors, patients, vendors, and suppliers; • Develop, test, and conduct educational training and awareness programs to reduce the likelihood of threat to the physical security of facilities; and • Implement, test, and update COOP, taking into account response and recovery across multiple threat scenarios into account.
Protection Against Insider Attacks or Disruptions	• Identify facility vulnerabilities to insider threats or other disruptions; • Develop a strategy for validating the identity of all workforce members, contractors, and volunteers; ensure that background checks on workforce members have been completed, giving special consideration to those staff with access to sensitive systems, areas, or functions associated with facilities; • Implement practices for authenticating vendors, suppliers, and other external visitors to facilities outside of normal hours; and • Implement, test, and update COOP with a focus on physical security protection.
Protection Against Natural or Manmade Occurrences	• Assess facility vulnerabilities to potential natural or manmade disasters or disruptions; • Develop a strategy and screening system for validating the identity of all workforce members, contractors, and volunteers; ensure that background checks on workforce members have been completed, giving special consideration to those staff with access to sensitive systems, areas, or functions associated with facilities; • Implement formal practices for authenticating vendors, suppliers, and others who may have access to facilities outside of normal hours (e.g., medical device vendors, outsourced IT management services, researchers); • Establish coordination links with local agencies to assure timely dissemination on potential threats to the physical structure of a facility; • Continuously update potential threats, such as severe weather warnings; • Develop and implement standards for conducting regular reviews of the physical structures of an organization, including, but not limited to, exterior access controls, monitoring systems, power systems, structural worthiness, adherence to Federal, State, and local code, and testing of systems intended to alert staff of a potential crisis (i.e., heat and cooling sensors, fire sensors, biological containment sensors, etc.); • Develop and implement appropriate training programs to ensure that staff recognize and understand the reporting requirements for adverse events; ensure that training covers workforce members, contractors, and volunteers; • Implement, test, and update COOP, taking into consideration processes for assessing the physical posture of the facility routinely and make the results available to facility management for action, if required.

Table 1-5: Long-Term Cyber Security Goals

Cyber Security Goals	Supporting Long-Term Objectives
Protection Against External Attacks	• Identify potential cyber threats, including, but not limited to, threats from hackers, virus attacks, worms, phishing, and social engineering attacks; • Conduct assessments to identify vulnerabilities in the network infrastructure associated with connections to the Internet, databases, servers, intranets, extranets, interconnections between business partners and gateway services, electronic health records, business processing systems, and the electronic architecture connecting these cyber assets within the facility; • Implement risk mitigation strategies for cyber threats, including electronic barriers to cyber attacks (e.g., firewalls, intrusion prevention/detection, configuration management tools, virtual local area network (VLAN) configurations, and access control and authentication mechanisms); • Establish, test, and conduct standardized cyber security training and awareness programs and refresher courses on a regularly scheduled basis; • Conduct tests of key technical resources (e.g., routers, switches, firewalls, modems) to expose vulnerabilities in the network infrastructure, making the results available to facility management for action, if required; • Establish requirements, policies, and procedures for locking and limiting resources based on user access requirements (e.g., Internet Protocol addresses, modems, wireless local area networks (LANs), and wireless resources); • Implement, test, and update COOP components, including requirements for information systems, utilities, facilities, and alert systems, taking into account response and recovery across multiple threat scenarios; and • Implement centralized incident response capability to identify and report, investigate and resolve cyber incidents, and apply appropriate disciplinary action, training, or guidance in response to incidents.
Protection Against Insider Attacks or User Negligence	• Identify and prioritize facility vulnerabilities to insider cyber attack, theft, and disruption; • Develop mechanisms to ensure that background checks on workforce members have been completed and validated, giving special consideration to staff with access to sensitive systems, areas, or functions associated with the facility; • Implement standardized practices for authenticating vendors, suppliers, and other external relationships that may have access to the facility outside of normal hours (e.g., medical device vendors, outsourced IT management services, emergency services units); • Implement appropriate electronic barriers to cyber attacks (e.g., firewalls, intrusion prevention/detection, configuration management tools, VLAN configurations, and access control and authentication mechanisms); • Test key technical resources (e.g., routers, switches, firewalls, modems) to expose vulnerabilities in the network infrastructure, making the results available to facility management for action, if required; • Implement access controls and auditing tools to detect and prevent rogue use of organizational data and information systems; • Establish requirements, policies, and procedures for handling, securing, and limiting resources based on user access requirements (e.g., IP addresses, modems, wireless LANs);

Cyber Security Goals	Supporting Long-Term Objectives
Protection Against Insider Attacks or User Negligence (continued)	• Establish and conduct standardized cyber security training and awareness programs and refresher courses on a regularly scheduled basis; • Establish failover or alternative processing sites for system failures; • Implement, test, and update COOP components, including requirements for information systems, utilities, facilities, and alert systems, taking into account response and recovery across multiple threat scenarios; and • Implement centralized incident response capability to identify and report, investigate and resolve cyber incidents, and apply appropriate disciplinary action, training, or guidance in response to incidents.
Protection against Natural or Manmade Disasters	• Assess network operations/data center vulnerabilities to potential natural or manmade disasters; • Assess Private Branch Exchange and other telecommunications systems for vulnerabilities to natural and manmade disasters, including single point of failure involving service provider, fire, smoke, water, freezing, chemicals, etc.; • Ensure that data back-ups and recovery plans are implemented and tested regularly; • Ensure that service-level agreements are reviewed, tested, and updated at regular intervals; • Develop a strategy for testing disaster recovery and continuity of operations plans; • Implement requirements for failover or redundant operations, including providing data recovery systems, conducting a business impact assessment, ensuring timely access to data back-ups, implementation at the alternate site of all packages required to conduct business processes, an accounting of staff functions and assigned staff for all critical functions, ensuring that staff have timely and safe access to alternate site locations, developing a vendor contact list for emergencies, ensure testing of any alternate processing sites and screening system for validation of all workforce members, contractors, and volunteers, etc.; • Implement formal practices for authenticating vendors, suppliers, and others who may have access to facilities outside of normal hours (e.g., medical device vendors, outsourced IT management services, researchers); • Establish coordination links with local agencies and emergency services to ensure timely response to adverse events and potential threats to the physical structure of a facility; • Continuously update potential threats, such as severe weather warnings; • Develop and implement standards for conducting regular testing of information and telecommunications systems, including failover and redundant systems; • Develop and implement appropriate training programs to ensure that staff recognize and understand the reporting requirements for adverse events; ensure that training covers workforce members, contractors, and volunteers; and • Implement, test, and update COOP, taking into consideration processes for business continuity.

1.4 Value Proposition

The value proposition for the Healthcare and Public Health Sector has three perspectives. From the National health perspective, sector functions must be protected because they are essential to the detection of, and response to, all incidents requiring emergency medical and public health services, and because they meet the daily healthcare and public health needs of the population during non-emergencies. The sector is uniquely qualified and irreplaceable for both of these functions.

From the sector's perspective, the continuing ability to perform its national mission is strengthened by sustainable, reliable protection of its CI/KR during crisis and non-crisis conditions.

From an economic perspective, the sector constitutes approximately 15 percent of GNP. Major disruptions to this sector could have cascading consequences across all other sectors and could create significant economic impacts to national economic security.

1.5 The Path Forward

In order to address the issues outlined in this section, the sector (GCC, SCC, and all relevant CI/KR protection partners) will need to undertake many tasks as the program matures. The list below addresses some of these. For the specific tasks to be undertaken in the coming year, please refer to the table in section 6.2, Implementation Actions.

1.5.1 The Sector Profile

Refine the sector profile to include any CI/KR protection-significant elements not taken into account in the SSP to date.

1.5.2 Goals and Objectives

Establish a joint GCC/SCC working group devoted to the goal-setting process, with responsibilities that include, but are not necessarily limited to, the following:

- Reviewing all available methodologies that could be used to help identify, characterize, and/or quantify goals, and implementing objectives for the sector;
- Reassessing the goals and objectives the sector has established for each of the major categories of sector assets;
- Modifying these goals and objectives as needed in light of additional information and experience with their planned or actual implementation in 2006; and
- Developing a preliminary strategy for implementing goals and objectives, particularly with respect to CI/KR protection.

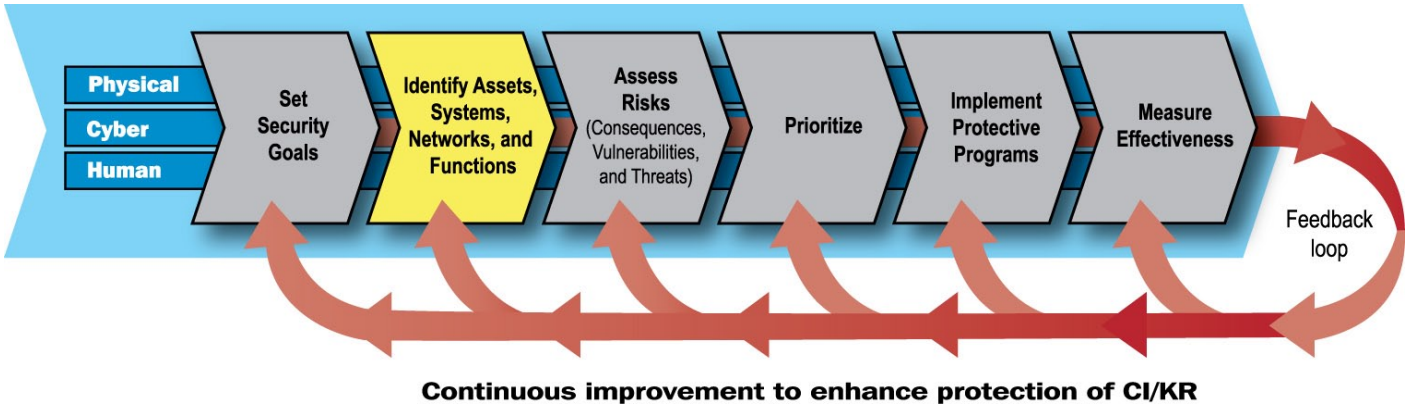
2. Identify Assets, Systems, Networks, and Functions

This section discusses infrastructure information collection methodologies to support sector CI/KR protection efforts. This description includes a discussion of asset data fields and other information parameters. It also describes how they align with the National Asset Database (NADB) infrastructure taxonomy developed by DHS and HHS with input from a panel of sector experts. Major topics in this section include the following:

- Defining information parameters;
- Collecting infrastructure information;
- Verifying infrastructure information;
- Updating infrastructure information; and
- The path forward.

The role this section plays in the overall DHS risk management program is summarized in figure 2-1.

Figure 2-1: The Role of Assets, Systems, Networks, and Functions



2.1 Defining Information Parameters

A simple listing of facilities or an industry breakdown does not capture the variety of assets, systems, networks, functions, and found in the sector. The sector is generally categorized in terms of health care (companies that develop, manufacture, market, and/or distribute health-related products or provide health care services, such as hospitals, nursing homes, or pay for care, such

as Health Maintenance Organizations (HMOs), as well as medical product suppliers, medical equipment and medical device makers, and medical laboratories) and life sciences (organizations in the fields of biotechnology, pharmaceuticals, biomedical technologies, environmental, and biomedical devices). Relationships can be described as many-to-many, with interdependencies tied to both economic and functional stability. The most commonly thought of asset in healthcare is the hospital. And, while large in numbers, they represent only a fraction of the total sector.

2.1.1 The Need for Multiple Parameter Systems

The sector's complexity in terms of size, scope, and relationships means that no single information parameter scheme is likely to be effective across the sector as a whole. It also means that identifying data characterizing CI/KR in useful ways is challenging. Numerous data classifications exist that may be helpful in characterizing sector assets; these include the NADB data definitions, the Industry Classification System Codes, Dun and Bradstreet numbers, U.S. Census Bureau classifications, and others.

2.1.2 Role of CI/KR in Information Parameter Development

Section 3 of this SSP identifies candidate CI/KR that will be evaluated for this designation in the coming year. This list, when finalized, will help define information parameters.

2.2 Collecting Infrastructure Information

Data collection across major sectors of the U.S. economy is subject to multiple Federal statutes. Appendix 3 identifies the major elements in the legislative framework relevant to this sector at the Federal level. In addition, sector elements are also subject to many State and local laws and regulations.

2.2.1 Assess Federal-Wide CI/KR Protection Legislative Requirements

Federal legislation has produced major changes across the Federal Government over the past 15 years. In addition to the requirements imposed by homeland security legislation, there are significant Federal statutes, regulatory programs, and security requirements facing nearly all the sectors. New requirements have had a broad impact on the establishment of protective programs. Examples are cited below of legislative requirements that HHS, VA, and DoD must satisfy with respect to CI/KR protection-related matters:

- The Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes requirements for the privacy and security of health data;
- The Public Health Threats and Emergencies Act (PHTEA) of 2000 authorizes the Secretary of HHS to take appropriate actions in the event of an infectious disease or bioterrorism attack;
- The Critical Infrastructure Protection Act (CIPA) of 2001 (Title III, Section 1016 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001) requires all Federal agencies to take certain steps to protect critical infrastructures under their control;
- The Cyber Security Enhancement Act (CSEA) of 2002 (Title II, Section 225 of the Homeland Security Act) requires all Federal agencies to take certain steps to protect automated IT systems under their control; and
- The Federal Information Security Management Act (FISMA) (Title III of the E-Government Act of 2002) requires that Federal agencies provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, including those provided or managed by another agency, contractor, or other source.

Appendix 3 provides additional information. Each of the above legislative items also has accompanying implementing regulations that must be assessed as well.

2.2.2 Preliminary Data List

Although the complexity of the sector presents significant issues from a data definition perspective, HHS has sketched a preliminary data set upon which to build. This data set includes the following broad topics:

- Basic identifying information for the asset, system, or network (e.g., name, location, owner or operator, principal contact for CI/KR protection matters);
- Principal functions;
- Nature of the operations supported by the asset, system, or network;
- Major dependencies and interdependencies facing the asset, system, or network;
- International considerations, if any;
- Existing protective measures in place; and
- Cyber elements and their connectivity to other cyber elements.

A next step is to define each of the above in terms supporting the development of specific data collection instruments.

2.2.3 Collecting Public Sector Data

Many of the CI/KR identified in the 2006 SSP are publicly controlled. As such, authorities may exist to encourage the collection and sharing of CI/KR protection-specific information. Still, assembling this information in one database will require considerable discussion among officials responsible for maintaining security. This process will be initiated in subsequent steps of plan development. Issues to discuss include, but are not limited to, the following:

- How to determine the precise information needed in order to avoid collecting data that will not have specific value;
- How to negotiate approval for the acquisition and use of Federal, State, local, tribal, and private sector data, if any, other than one jurisdiction or facility at a time;
- How to integrate data from disparate sources and variable formats into a coherent whole that will serve useful purposes;
- How to update the data on a recurring basis at an acceptable cost to all concerned;
- How to limit data access based on need-to-know or other appropriate tests;
- How to address Office of Management and Budget (OMB) approval for data collection under the Paperwork Reduction Act and other statutory guidance;
- Timeframe for data collection processes;
- Parties responsible for coordinating data collection;
- Sources of asset data (e.g., owners and operators, State and local governments, industry associations, commercial sources);
- Use of standardized terminology so that data collected from all sectors is consistent and uniform;
- Status of current asset data collection efforts; and
- Defining relevant information protection issues related to each process for each data source.

2.2.4 Collecting Private Sector Data

In addition to sharing many of the issues that affect the collection of public sector data, the challenge of private sector data collection is compounded by several factors. Private sector entities are not necessarily obligated by law or regulation to provide the CI/KR-related information required under the NIPP. Within the sector, all private sector entities understand they will be responders to terrorist attacks or natural disasters, but only a few regard themselves as a primary (or even potential) target for terrorism. Few have direct experience with healthcare or public health organizations as terrorist targets; most do have experience with natural disasters.

Many leaders of private healthcare entities, therefore, may be reluctant to commit time and resources to assessing the vulnerability of their enterprises to direct attacks on their physical or cyber infrastructures. Perhaps equally important, most do not yet see how the Federal Government can assist them in ways other than direct funding or expense reimbursements.

Finally, there are Federal regulations that affect the sharing of certain information. For example, HIPAA restricts the unauthorized use or disclosure of individually identifiable health information that health plans, healthcare clearinghouses, and healthcare providers receive, maintain, create or transmit.

Despite these challenges, in 2006, DHS and HHS reached out to private sector and State and local partners to collect data for inclusion in the NADB. Though results were mixed, one lesson learned was the need for better integration of plans at different levels of government to reduce the data collection burden. An added advantage as the 2007 effort begins is the finalization of the updated rule for the handling and collection of Protected Critical Infrastructure Information (PCII). HHS is in the process of developing improved procedures for using the rule and making the program better known to its security partners.

2.2.5 Information Already Available on Sector and Cross-Sector Assets

Sector-specific information used in earlier versions of the SSP has been drawn from a variety of public sources. These sources include data published by Federal agencies, articles by reputable authorities, governmental studies, information published on Web sites by professional organizations working in the field, comments by HHS reviewers on drafts of the SSP, and official statements and/or studies by professional associations within the sector. In short, a vast amount of data on this sector is already available that could be used more effectively. Before data collection begins, however, data elements under consideration must be analyzed to meet the following five tests:

- Relevance and usefulness from a CI/KR protection perspective;
- Availability at a reasonable cost both to those collecting and those providing the data;
- Collection within the legal authority under which the data is requested;
- Comparability from one facility to another within a given category of facility; and
- Alignment with the NADB infrastructure taxonomy developed by DHS and the SSAs.[26]

Because it is more efficient to use information that already exists, HHS is currently working to identify the best way to incorporate data in the most effective manner.

2.2.6 Asset Information Protection Mechanisms

Until the candidate CI/KR identified in this section of the SSP have been properly adjudicated by HHS, the GCC, and the SCC, information characterizing them in detail is not included in this SSP. Instead, they are described in summary terms. When the

[26] Required by DHS, 2006 Critical Infrastructure/Key Resources Protection Sector-Specific Plan Guidance, Section 2, March 31, 2006.

final list of CI/KR is established, detailed information on each will be housed at appropriate locations (e.g., HHS headquarters, the Centers for Disease Control and Prevention (CDC)) in protected storage under HHS auspices. If detailed information is required, HHS will provide DHS with such information on a case-by-case basis.

2.3 Verifying Infrastructure Information

Where possible, all data will be collected directly from the relevant managers, owners, or operators of CI/KR and verified by them. This should ensure that the collected data is accurate and approved for use in SSP development by those understanding the relevant issues surrounding data collection involving the facility or function in question. The following issues must also be resolved beforehand:

- How to process incomplete and/or inaccurate data;
- The follow-up activities needed based on the significance of the asset, system, or network (e.g., on-site meetings, validation of owner/operator procedures); and
- Any special verification steps that must be taken to account for the differences in data relating to physical, cyber, and/or human elements.

2.3.1 Verifying Asset Data

As just noted, HHS will obtain the majority of the required data directly from the managers of the assets, systems, networks, and functions involved. Using these trusted sources should ensure that the data is verified.

2.3.2 Reviewing Data

Since the data received from relevant facility managers, owners, or operators can be viewed as authoritative, it will not be reviewed for accuracy by HHS (apart from transmission or transcription errors). If data obtained from private sector facility Web sites is date stamped, the Web site managers can be contacted to obtain verification of currency and accuracy.

2.3.3 Protocol for Reviewing Data

All information collected on CI/KR will be reviewed for completeness and accuracy using systematic data review processes. No sampling processes will be used; instead all information collected on CI/KR will be reviewed in its totality. Depending on the data elements finally chosen, reviews will employ standard techniques for assessing data quality (e.g., checking for blanks, unexpected entries, values falling outside of expected ranges, dramatic differences between values report in one period versus another). When the appropriate data sets are identified, explicit data checks will be devised.

2.3.4 Steps to Address Incomplete and/or Inaccurate Data

After review for completeness and accuracy, if data appears to be missing or incomplete, the appropriate steps will be taken to resolve these discrepancies. These steps will include, but not necessarily be limited to, contacting the provider/source of the information to obtain validation.

2.4 Updating Infrastructure Information

As the 2006 DHS guidance acknowledges, all CI/KR data is subject to change over time. Data will be updated by surveying appropriate owners and operators. This data survey will request that key information be updated from the prior year on an exception basis (i.e., reporting changes only).

2.4.1 How Updated Information Will Be Provided

Nearly all CI/KR information described in this SSP is subject to reevaluation in light of changing circumstances. This reevaluation will occur annually in connection with the SSP update required by HSPD-7. However, unforeseen events may mandate earlier updates (e.g., impending threats or real-world incidents, natural or manmade).

2.4.2 Frequency of Data Submission

To a great extent, appropriate frequency of data submission varies by circumstance. Some information is subject to rapid obsolescence (e.g., key contact information for individuals). Other information is less prone to obsolescence (e.g., key services provided by a given asset, system, network, or function). Still other information changes infrequently, but at unpredictable times from one facility to another (e.g., the geographic location of a given facility). For these reasons, there is no single frequency that is 'best' for updating all information. At a minimum, data will be collected/updated on an annual basis. This data survey will request that key information be updated from the prior year on an exception basis (i.e., reporting changes only).

The frequency of submission will be based upon the recommendations of the GCC and the SCC. Both can provide mechanisms for ensuring appropriate lines of communication, and for clarifying contrasting viewpoints on key CI/KR issues of joint interest.

2.4.3 Notifying DHS of Data Updates

Procedures for updating information discussed in this section will be defined after HHS has accumulated some experience with data quality issues.

2.4.4 SSA Office Responsible for Obtaining the Data

ASPR is responsible for this task. For data collection involving Federal agencies, HHS ASPR will work with those agencies directly through the GCC. For State, local, and tribal bodies, ASPR will work through its public sector partners. For private sector data, ASPR will work through the SCC and various professional bodies identified by the SCC.

2.4.5 Maintaining Data

HHS ASPR is responsible for collecting and maintaining data. It will establish an appropriate data system for this purpose at HHS headquarters. For data collection involving Federal agencies that wish to maintain their own data, ASPR will work with those agencies to ensure that information can be shared in the most efficient manner. In addition, ASPR will coordinate with NADB and Homeland Security Information Network (HSIN) personnel to ensure that information storage systems are used efficiently and that asset information stored in these systems is consistent.

2.4.6 Information Protection Mechanisms for NADB and SSA Information Sharing

Data collection mechanisms must be informed by the requirement to be in alignment with the NADB. This requirement will be met through continuing discussions with NADB staff as the NADB continues to evolve.

The Homeland Security Act created a category of information that, when submitted to the Federal Government, can be protected from public disclosure under the Freedom of Information Act (FOIA), State and local sunshine laws, and civil litigation proceedings. Voluntarily submitted by private sector entities, this information is called PCII.[27]

[27] See Homeland Security Act of 2002, 6 United States Code (U.S.C.) 133, Section 214.

Final rules for handling such information are contained in *Procedures for Handling Critical Infrastructure Information.*[28] These procedures govern the receipt, validation, handling, storage, marking, and use of critical infrastructure information voluntarily submitted to the DHS. The procedures are applicable to all Federal, State, local, and tribal government agencies and contractors that have access to, handle, use, or store critical infrastructure information that enjoys protection under the Critical Infrastructure Information (CII) Act of 2002.

Procedures for dealing with PCII information within the sector are being defined as HHS accumulates sufficient experience with PCII-protected data.[29]

2.5 The Path Forward

In order to address the issues outlined in this section, the sector (GCC, SCC, and all relevant CI/KR protection partners) will need to undertake many tasks as the program matures. The list below addresses some of these. For the specific tasks to be undertaken in the coming year, refer to the table in section 6.2, Implementation Actions.

- Assess available data classification sets for their availability and relevance to HSPD-7 objectives and requirements;
- Identify data that are already collected and could be used to meet HSPD-7 requirements in the sector after assessing the statutory requirements for data reporting for major sector entities;
- Assess procedures identified in this SSP for collecting, validating, and updating CI/KR protection-related data to assure that these procedures are cost-effective, meet all HSPD-7 needs, and are not burdensome on entities charged with providing data;
- Evaluate the need for additional procedures to handle PCII or other sensitive data in the event that procedures are authorized for its collection and use by HHS; and
- Develop a plan for CI/KR protection-related data collection in consultation with the GCC, the SCC, and other sector strategic partners that meets all requirements.

[28] See 71 Federal Register (FR) 170, September 1, 2006, DHS, Office of the Secretary, Procedures for Handling Critical Infrastructure Information, which establishes uniform procedures for implementing the Critical Infrastructure Information Act of 2002.

[29] The Final Rule deals only with PCII information submitted to DHS (i.e., "direct" information). The program will likely be expanded to operate with Federal agencies other than DHS on an "indirect" basis at some point in the future. See Department of Justice, Office of Information and Privacy, FOIA Post, www.usdoj.gov/oip/foiapost/2004/foiapost6.htm.

3. Assess Risk

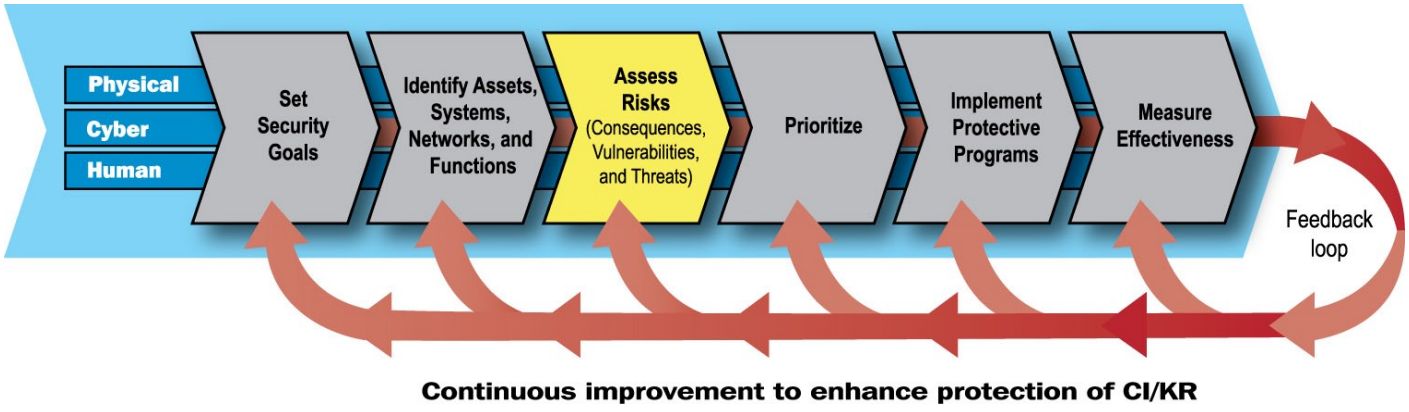
This section outlines overall risk assessment planning within the Healthcare Sector to date. This section also outlines sector plans for analyzing risks with a view toward establishing a tailored risk management framework consistent with DHS guidance. Risk assessments are a necessary activity for implementing mitigation strategies and increasing the sector's overall security posture. Risk assessments will generally analyze vulnerabilities against known threats, thus allowing the sector to look at risks in terms of high, medium, and low thresholds in terms of the ability to exploit the vulnerabilities and estimate or quantify the resulting consequences. Major topics in this section include the following:

- Use of risk assessment in the sector;
- Screening infrastructure;
- Assessing consequences;
- Assessing vulnerabilities;
- Assessing threats; and
- The path forward.

3.1 Use of Risk Assessment in the Sector

The Healthcare and Public Health Sector acknowledges the DHS-prescribed risk management framework and its risk assessment activities fit the DHS risk management framework. This framework is summarized below.

Figure 3-1: Assess Risks, Consequences, Vulnerabilities, and Threats



According to the NIPP, risk is a function of consequence, vulnerability, and threat.[30] Risk is the expected magnitude of loss due to terrorist attack, natural disaster, or other incident, together with the likelihood of such an event occurring and causing that loss. In formula terms, risk (R) can be expressed as:

Risk (R) = f(Consequences (C), Vulnerability (V), Threat (T))

Where:

C = Consequences. Consequences are expressed as the negative effects on public health and safety, the economy, public confidence in institutions, and the functioning of government, both direct and indirect, that can be expected if an asset, system, or network is damaged, destroyed, or disrupted by a terrorist attack, natural disaster, or other incident.

V = Vulnerability. Vulnerability is expressed as the likelihood that a characteristic of, or flaw in, an asset, system, or network's design, location, security posture, process, or operation renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional acts, mechanical failures, or natural hazards.

T = Threat. Threat is expressed as the likelihood that a particular asset, system, or network will suffer an attack or an incident. For terrorist attacks, this likelihood is judged from the intent and capability of an adversary. For natural disasters or accidents, the likelihood is based on the probability of occurrence.[31]

The implementation of the NIPP risk management framework in the Healthcare and Public Health Sector requires several elements as follows:

- Screening the vast number of assets, systems, and supporting workforce members in the $1.9 trillion Healthcare and Public Health Sector to identify candidate CI/KR for further review;
- Obtain integrated view of sector risk assessments sector-wide by cataloging the risk-reduction activities already in place;
- Conducting assessments of the vulnerabilities facing each CI/KR selected from the initial screening; and
- Developing a suggested protocol to assess procedures employed for reducing or eliminating vulnerabilities suitable for use by on-site security officials and site visitors at all levels.

Table 3-1 outlines the overall objective, entity responsible, and relevant sections of the SSP for each element.

[30] See Department of Homeland Security, National Infrastructure Protection Plan, Section 3.3, Assess Risks, June 30, 2006.

[31] These definitions are drawn from DHS, National Infrastructure Protection Plan, Section 3.3, Assess Risks, June 30, 2006.

3.2 Screening Infrastructure

The first of these elements is initial screening. As the DHS guidance for 2006 points out, performing a risk assessment on an asset, system, network, or function can require significant resources. Full assessments may not be justified in all cases.[32] After 2 years of investigation, and taking the size, scope of services, and disparities between organizations into account, HHS identified two screening methods for determining the current candidate critical assets, systems, and workforce. Both produced nearly identical results.

Table 3-1: Four Elements in Identifying, Assessing, and Protecting CI/KR in the Healthcare and Public Health Sector

Elements	Perform Initial Screen	Obtain Integrated View of Sector Risk Assessments Sector-Wide	Perform Risk Assessments	Develop Risk Reduction Processes Documenting Best Practices
Overall objective	Review sector as a whole to identify candidate CI/KR for detailed examination	Assemble complete view of all assessments being made regardless of mandate	Conduct formal risk assessments of agreed-upon CI/KR	Equip security officials, site visitors, and others with the procedures to assess the effectiveness of risk-reduction and mitigation efforts, building on existing public and private sector procedures
Entities primarily responsible	SSA in consultation with its GCC and SCC representatives	SSA, GCC, and SCC	SSA, in consultation with CI/KR managers, owners, operators, and relevant private sector entities	Public sector security officials with CI/KR protection responsibilities for CI/KR and private sector security managers with CI/KR protection responsibilities
Relevant sections of this SSP	Section 3	Sections 4 and 5	Sections 3, 4, and 5	Appendix 5

3.2.1 Scenario-Based Screening

This method assessed candidate critical assets, systems, or networks against the 15 Homeland Security Council (HSC) planning scenarios published in 2003.[33] Ten of these scenarios involved a terrorist attack, four involved natural events, and one involved a cyber attack. The more scenarios in which a candidate plays a significant protection, response, or mitigation role, the stronger its case for designation as a CI or KR.[34]

[32] See DHS, 2006 Critical Infrastructure/Key Resources Protection Sector-Specific Plan Guidance, March 31, 2006, Section 3: Assess Risks, Section 3.2, Screening Infrastructure, p. 18.

[33] These scenarios included: (1) a 10-kiloton nuclear explosion; (2) an aerosol anthrax attack; (3) a naturally occurring pandemic influenza event; (4) a terrorist attack using plague; (5) terrorist blister agent attack on a stadium; (6) terrorist attack using toxic industrial chemicals; (7) terrorist attack using nerve agent; (8) terrorist-induced chlorine tank explosion; (9) major earthquake; (10) major hurricane; (11) terrorist "dirty bomb" attack; (12) terrorist use of a conventional explosive device; (13) natural or induced food poisoning outbreak; (14) natural or induced foot-and-mouth disease outbreak; and, (15) cyber attack against various systems. See The Homeland Security Council, Planning Scenarios Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities, Executive Summary, Version 2.0, July 2004.

[34] For a detailed description of this methodology, see HHS, Draft Sector Specific Plan for the Healthcare and Public Health Sector: An Element of the National Infrastructure Protection Plan, December 31, 2005, Section 3, A.1.

3.2.2 Functionally Based Screening

This method employed seven functional criteria to assess candidates.[35] These criteria concentrated on a given asset's national importance from several perspectives. The more functional criteria a candidate satisfied, the stronger its case for designation as a CI or KR.[36]

To the extent practical, both screening methods conformed to prescriptions in Annex 4 of the guidance.

3.2.3 Resulting Candidate CI/KR

These two methods produced a list of candidates for detailed review. For further information on candidate CI/KR, please contact the Department of Health and Human Services Office of the Assistant Secretary for Preparedness and Response.

3.2.4 Existing Risk Assessments in the Sector

The second element in the sector's strategy is surveying the CI/KR protection-related assessments already being conducted across the sector, identifying gaps, and helping promote greater integration. HHS and its public sector security partners currently conduct significant assessments or encourage the development of protective programs. These efforts result from various mandates such as meeting HSPD-7 requirements. Private sector entities also conduct such assessments and programs in response to a variety of imperatives, such as accreditation and regulatory requirements. These assessment and protective programs are summarized in section 5.1 of this SSP.

3.2.5 HHS-Sponsored Methodology Reviews

The third element in the overall approach is to develop methods that can be used to perform detailed assessments of agreed-upon CI/KR. Last year, HHS reviewed 67 risk and vulnerability assessment tools and methodologies for applicability in the CI/KR protection context.[37] HHS representatives also attended technical assistance sessions sponsored by DHS during the past year. In consultation with DHS, HHS identified vulnerabilities that are known or that are believed to face the sector as a whole.[38]

Based on the results, several methods could be used by personnel throughout the sector, all of which are summarized in Appendix 4 of this SSP. These methods will be assessed for relevance, utility, and conformance to principles listed in Appendix 3A of the NIPP in the upcoming year.

[35] These criteria include the following: (1) the degree of geographical dispersion that is characteristic of the CI or KR, since everything else being equal, the greater the dispersion, the lower the risk associated with their destruction or incapacitation; (2) the number of suppliers of the CI or KR since everything else being equal, the fewer the suppliers, the greater the risk associated with their destruction or incapacitation; (3) the extent to which the CI or KR supplies critical knowledge (i.e., specialized knowledge playing major roles in responding to healthcare or public health threats), since the more CI/KR are a source of critical knowledge, the greater the risk associated with their destruction or incapacitation; (4) the degree to which the CI or KR is critical to mounting region-wide responses to emergencies; (5) the degree to which the CI or KR are critical to mounting national responses to emergencies; (6) the degree to which the CI or KR provide (or help provide) an early warning capability for emerging healthcare or public health threats; and (7) a summary of the overall impact of the loss of the CI or KR based on the criteria above (rated as high, medium, or low).

[36] See The Homeland Security Council, Planning Scenarios Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities, Executive Summary, Version 2.0, July 2004. For a detailed description of this methodology, see HHS, Draft Sector Specific Plan for the Healthcare and Public Health Sector: An Element of the National Infrastructure Protection Plan, December 31, 2005, Section 3, A.2.4.

[37] These included 25 high-level tools and methodologies and 14 cyber-oriented tools, methods, and standards. High-level tools included: (1) Risk Assessment Methodologies for Use in the Electric Utility Industry (Review Draft); (2) Australia/New Zealand Risk Management Guidelines; (3) PNNI, Risk Communication Assessment and Prioritization Program; (4) American Electric Power Attack Tree Methodology; (5) Risk Assessment Methodology for Dams and Electric Transmission; (6) EEI Security Committee Approach to Risk/Vulnerability Assessment; (7) Building for Environmental and Economic Sustainability; (8) Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability + SHOCK; (9) Hospital Emergency Analysis Tool; (10) Security Code of Management Practices for Physical and Cyber Security Activities; (11) Design Assurance Red Team; (12) INFOSEC Assessment Methodology; (13) International General Security Risk Assessment Guideline; (14) Natural Disaster Mitigation in Drinking Water and Sanitation Systems: Guidelines for Vulnerability Analysis; (15) Physical Security Assessment for Department of Veterans Affairs Facilities; (16) Project Matrix and Its Function, Service and Product Evaluation Tool; (17) Vulnerability Risk Analysis Program; (18) ASME Risk Analysis and Management for Critical Asset Protection; (19) Department of Defense Standard Practice for System Safety; (20) Balanced Survivability Assessments; (21) TAME: Threat Assessment Model for the METEORE System; (22) Toward a Secure Systems Engineering Methodology; (23) Vulnerability Assessment Methodology for U.S. Chemical Facilities; (24) Vulnerability Assessment Survey Program: Overview of Assessment Methodology; and (25) Wholesale Medical Logistics Readiness Plan. Cyber-oriented tools and methodologies included: (1) Tools, Standards and Publications for Assessing the Security of Automated Systems Published by the National Institute of Standards and Technology (29 entries); (2) Some Representative Tools, Standards, or Publications for Assessing Automated Systems Listed Alphabetically by Various Authorities (8 items); and (3) Selected International Organization for Standards (ISO) Standards Related to IT Security (5 entries).

[38] See HHS, Draft Sector Specific Plan for Critical Infrastructure Protection in the Healthcare and Public Health Sector, Section 4, December 31, 2005.

3.2.6 Development of Draft Best Practices for Assessments of Protective Mechanisms

The fourth element is a draft set of best practices for on-site CI/KR protection-related security assessments. After evaluating all available information, HHS prepared a draft evaluation protocol that could be used to assess the effectiveness of security procedures intended to protect facilities, computer information systems, and workforce personnel. This draft evaluation protocol can be applied by owners, operators, and government assessment personnel anywhere in the sector, not just to CI/KR.

3.2.7 Classification of Aggregated CI/KR Information

For further information regarding the classification of the Aggregated CI/KR information, please contact the Department of Health and Human Services Office of the Assistant Secretary for Preparedness and Response.

3.3 Assessing Consequences

As defined in the NIPP, consequences are the negative effects on public health and safety, the economy, public confidence in institutions, and the functioning of government, both direct and indirect, that can be expected if an asset, system, network, or function is damaged, destroyed, or disrupted by a terrorist attack, natural disaster, or other incident.[39]

3.3.1 Use of SHIRA

As required by DHS, HHS is employing the Strategic Homeland Infrastructure Risk Assessment (SHIRA) methodology to assess consequences to sector assets. The SHIRA methodology takes a high-level approach to identifying those assets, functions, and systems that would have a national impact were they attacked, focusing on both the direct consequences to the sector and the cascading consequences that would likely result in catastrophic effects. The analysis centers on potential outcomes related to loss of life, economic losses, and behavioral impacts that are the result of strategic vulnerabilities associated with CI/KR. To ensure consistency across all sectors, the SHIRA process is based on a series of pre-defined threat scenarios. Using the SHIRA methodology, HHS is assessing and ranking consequences in two areas:

- Consequences related to the Healthcare and Public Health Sector; and
- Cascading consequences related to other sectors, to the extent feasible, to help forecast response efforts, reduce recovery timeframes, and assist the return to normal operations.

Results from the SHIRA methodology are intended to provide information that supports sector and security partner responses to emergent threats or immediate incidents, and the strategic planning needed to enhance the protection of U.S. CI/KR over the long term. Once the SHIRA assessment rating has been completed, the resulting data may be made available to sector security partners, as appropriate. It will also be evaluated for integration into national and local risk assessment activities.

Table 3-3 suggests examples of likely consequences in the SHIRA analysis categories identified during discussions with sector security partners in 2006.

3.3.2 Factors Prompting Sector Resilience

The vast number of healthcare and public health assets nationally assures many regional and local redundancies. These redundancies provide significant resilience within the sector. Thus, while all sector assets are locally important, the loss or incapacitation of any single asset, or local cluster of assets, would typically not result in significant national consequences.

[39] See DHS, National Infrastructure Protection Plan, Section 3.3, Assess Risks, June 30, 2006, p. 35.

Table 3-2: Possible Consequences of Exploiting Vulnerabilities in the Healthcare and Public Health Sector[40]

Dimension	Possible Consequences
Loss of life, illness, and injury	• Primarily local, limited impact, except in a major natural disaster, biological attack, or nuclear detonation; • Impairment of response capabilities for a bioterrorism attack or pandemic could spread to the regional or national level; • The National healthcare and public health system workforce would not be crippled in most scenarios, but could be by a catastrophic bio-attack or an unchecked pandemic; and • Interdependence with the water system, the transportation network, the electrical power grid, the food chain, and civil authorities could raise safety issues for healthcare and public health workers.
Economic impact	• Primarily local impacts in most scenarios; • In cases not involving a catastrophic natural disaster, bio-attack, or pandemic, the geographically dispersed nature of the sector largely precludes national impact; • Significant local or regional economic impacts are possible; and • Dependence on the water system, the transportation network, the electrical power grid, the food chain, and the effectiveness of civil authorities could create economic dislocations, perhaps rising to regional significance.
Psychological and behavioral impacts	• Attack on an entity with high symbolic national value could affect national morale in the short term (but might strengthen public resolve in the longer term); • A catastrophic bio-event or natural disaster could have widespread, long-lasting effects on behavior; and • Otherwise, limited local impact to the surrounding area seems likely.

3.4 Assessing Vulnerabilities

The next step in the risk assessment process is to characterize the vulnerabilities to which the sector is susceptible. According to the NIPP, vulnerability is the "likelihood that a characteristic of, or flaw in, an asset, system, or network's design, location, security posture, process, or operation renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional acts, mechanical failures, and natural hazards.[41]

3.4.1 Available Templates

CI/KR assets vary with respect to CI/KR protection-related characteristics. As a result, there is no template of vulnerabilities applicable to all assets within a given sector. A general list includes vulnerabilities regarding the following:

- Cyber attacks against electronic information systems and networks;
- Physical attacks against facilities using chemical, biological, radiological, or sniper weapons;

[40] From discussions with sector reviewers as documented in HHS, Draft Sector Specific Plan for the Healthcare and Public Health Sector: An Element of the National Infrastructure Protection Plan, Section 4, December 31, 2005, and reviewer comments in 2006.

[41] See DHS, National Infrastructure Protection Plan, Section 3.3, Assess Risks, June 30, 2006, p. 35.

- Disruptions of functions, systems, and facilities by insider individuals or insider/outsider collaborators;
- Disruptions to functions, systems, and facilities caused by natural disasters (e.g., fires, floods, earthquakes, tornados, hurricanes);
- Disruptions due to naturally occurring bio-events (e.g., SARS, pandemic disease outbreaks); and
- Patient surges due to explosions, chemicals, biological attacks, or natural disasters.[42]

The likelihood of each of these vulnerabilities differs and is not estimated in this SSP. Drawing upon a detailed discussion of these vulnerabilities in the 2005 SSP, and subsequent discussion with sector security partners in 2006, these vulnerabilities will be defined in further detail in 2007.

3.4.2 Vulnerability Components

The DHS has identified several models for determining the likelihood of an attack's success. The Healthcare and Public Health Sector is considering scenarios and assessment tools that look at vulnerabilities in terms of the following components:[43]

- Ability of the adversary to identify the asset and its criticality;
- Likelihood that the countermeasures in place will prevent the attack from succeeding; and
- If countermeasures fail, the likelihood that the attack will still have the desired effect (robustness, resistance, and resilience of the target).

At a high level, table 3-4 summarizes possible vulnerabilities thought to be facing some, if not all, of the Healthcare and Public Health Sector. Further exploration of their applicability to CI/KR identified in 2007 will be required.

3.4.3 Vulnerability-Oriented Tools Oriented Toward Information Technology

Numerous approaches in the IT industry are available to assess cyber risks and vulnerabilities. These have varying degrees of utility in the CI/KR protection context, depending on their purpose and other factors.[44] Some are specific to an application or database. Others apply to computer operating systems. Still others have a system-wide perspective.[45] HHS has reviewed 14 such plans, tools, or methodologies focusing on automated systems, networks, and procedures. Some are widely used within the Healthcare and Public Health Sector already.[46] These are summarized in Appendix 4 of this SSP.

[42] See HHS, Draft Sector Specific Plan for the Healthcare and Public Health Sector: An Element of the National Infrastructure Protection Plan, Section 4, December 31, 2005.

[43] DHS Strategic Homeland Infrastructure Risk Assessment Vulnerability Model, July 3, 2006.

[44] Communication from the Information Technology Coordinating Group offering technical advice to the HHS Office of Public Health Emergency Preparedness, January 5, 2005.

[45] Ibid.

[46] Examples of tools widely used include OCTAVE, ODP-SNJTK, RAMCAP, RelSec, and RiskWatch. In addition, many tools are oriented toward automated systems only. Many such tools adhere to national standards such as the National Institute of Standards and Technology 800 Series Publication, as well as international standards such as ISO 11799.

Table 3-3: Possible Healthcare and Public Health Sector Threats by Major Type[47]

Type	Possible Examples
Cyber attacks against electronic systems and networks	• Computer malware potentially affecting any IT system; • Disgruntled insider attacks resulting in information systems disruptions; • Externally based hacker attacks against routers, switches, and firewalls resulting in disruptions to the network infrastructure; and • Attacks at the application level rendering services or systems inoperable.
Physical attacks against fixed facilities[48]	• Vehicle or suicide bomb attacks; • Armed attacks; and • Disgruntled insider attacks with or without outsider collaborators.
Disruptions by individuals, including insiders and insider/outsider combinations	• Insider physical attacks; • Insider theft or destruction of intellectual property; and • Insider/outsider attacks employing physical and/or cyber methods.
Other vulnerabilities	• Natural disasters; • Naturally occurring bio-events; • Threats to clinical staff from patients infected elsewhere seeking treatment; • Communications and transportation interruptions; • Surge capacity vulnerabilities; • Uncontrolled/unexpected public reaction to attacks/disasters; • Lack of resources for vulnerability-reduction programs; • Labor disputes or disruptions; and • Intelligence gaps resulting in shortened response time availability.

3.5 Assessing Threats

DHS guidance requires that the SSP describe the general threat environment for the sector.[49] According to the NIPP, threat is "the likelihood that a particular asset, system, or network will suffer an attack or an incident. In the context of a risk from terrorist attack, the estimate of this is based on the analysis of the intent and the capability of an adversary. In the context of natural disaster or accident, the likelihood is based on the probability of occurrence."[50] The Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) has characterized this process in terms of five major tasks for the country as a whole.

3.5.1 General Threat Description

For 2007, HHS will coordinate with DHS HITRAC to produce suitable versions of HITRAC products for use, as appropriate, when sharing information with private sector security partners. The following is an overall summary of threats facing the sector.

[47] From discussions with sector reviewers as documented in HHS, Draft Sector-Specific Plan for the Healthcare and Public Health Sector: An Element of the National Infrastructure Protection Plan, Section 4, December 31, 2005, and reviewer comments during 2006.

[48] Physical attacks might be motivated by the desire to damage a facility, affect the ability of a facility or locality to deliver care or to procure dangerous materials stored at the facility, etc.

[49] Section 4 of the 2005 SSP describes in detail threats to which the sector is especially vulnerable.

[50] See DHS, National Infrastructure Protection Plan, Section 3.3, Assess Risks, June 30, 2006, p. 35.

3.5.1.1 Cyber Attacks Against Electronic Systems and Networks

The Healthcare and Public Health Sector is not as reliant on IT and systems as some other sectors. However, that is changing rapidly and cyber threats to the Healthcare and Public Health Sector do exist and are likely to increase if appropriate steps are not taken. Table 3-5 summarizes the types of cyber attackers most commonly observed across all sectors, together with a summary of the threats most commonly associated with each. Table 3-6 summarizes major tools used by cyber attackers. These tools could be used against cyber assets in all sectors.

Table 3-4: Types of Cyber Threats to Critical Infrastructures Observed by Federal Authorities[51] (Listed Alphabetically)

Threat	Description of Threat
Bot-network operators	Taking over multiple systems to coordinate attacks and to perpetrate phishing schemes, spam, and malware attacks.
Criminal groups	Cyber intrusions by criminal groups (e.g., domestic extremist groups) that attack systems for monetary gain.
Foreign intelligence services	Use of cyber tools as part of continuing information-gathering and espionage activities.
Hackers	Hacking into networks for the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill and/or computer knowledge, hackers can now download attack scripts and protocols from the Internet. Attack tools have become more sophisticated and have also become easier to use.
Hacktivists	Politically motivated attacks on publicly accessible Web pages or e-mail servers. Hacktivist groups/individuals overload e-mail servers and hack into Web sites to send political messages.
Information warfare	Disrupting the supply, communications, and economic infrastructures that support national power by attacking supporting computer systems. Several nations are aggressively working to develop information warfare doctrine, programs, and capabilities.
Insider threats	Disgruntled worker or infiltrated persons causing damage to the organization's computer systems or stealing system data. Insiders may be the principal source of computer crime due, in part, to their detailed knowledge of the systems they attack.
Phishers	Web-based schemes in which financial criminals send electronic messages to unsuspecting users posing as a genuine business requesting "verification" of key financial/identification information that can be used in fraud schemes.
Radio-frequency weapons	Use of radio-frequency weapons to disrupt and/or terminate IT and processing capabilities used by a facility.
Spammers	Distribution of unsolicited e-mail with hidden or false information to sell products legitimately; conduct phishing schemes; distribute spyware, malware, or attack organizations.
Terrorists	Terrorists seeking to destroy, incapacitate, or exploit critical infrastructures to threaten National security, cause mass casualties, weaken the economy, and/or damage public morale or confidence.
Virus writers	Preparation and transmission of destructive computer viruses and "worms" that harm files and hard drives (e.g., the Melissa Macro Virus, the Explore.Zip worm, the Chernobyl Virus, Nimda, and Code Red).

[51] Adapted from Robert F. Dacey, Director, Information Security Issues, General Accounting Office, in testimony before the Subcommittee on Cyber Security, Science, and Research and Development and the Subcommittee on Infrastructure and Border Security, Select Committee on Homeland Security, U.S. House of Representatives, Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues, GAO-03-1165T, September 17, 2003, and DHS HITRAC office during 2006.

Table 3-5: Common Tools Used in Cyber Attacks[52] (Listed Alphabetically)

Attack Type	Description
Denial of service	Overwhelming a target computer with messages that block legitimate traffic and interfere with normal functioning.
Exploit tools	Publicly available tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bomb	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs (e.g., terminating the programmer's employment).
Phishing	Use of e-mail and Web sites disguised as legitimate businesses or public agencies to entice users into disclosing personal information that can be used to defraud.
Sniffer	Synonymous with packet sniffer, a program that intercepts routed data and examines each packet in search of specified information (e.g., passwords transmitted in clear text).
Trojan horse	A computer program that conceals harmful code, but masquerades as a useful program that a user would wish to execute.
Virus	A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human action (usually unwitting) such as clicking on an e-mail attachment to propagate.
War dialing	Programs that dial consecutive telephone numbers looking for modems to penetrate for illegal purposes.
War driving	Patrolling geographic locations with antennas looking for wireless computer networks to penetrate for illegal purposes.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate

These threats and tools evolve rapidly given the ingenuity of the cyber attacker community. With some exceptions, all can be blocked by continuously updated computer security programs. Such programs include adherence to procedural safeguards for the system; an effective, continuously adaptive firewall; the application of intrusion detection/intrusion prevention systems for detecting, reporting, and preventing external threats to the network and information systems; surveillance programs for detecting insider threats; continuing training of users of the system concerning proper security procedures; use of passwords resistant to hacker compromise; and related safeguards.

3.5.1.2 Physical Threats

The greatest day-to-day terrorist threat around the world continues to be attacks using conventional explosives. Much less frequent to date, but potentially more serious, are attacks using chemical, biological, or radiological dispersion agents.

[52] Adapted from Robert F. Dacey, Director, Information Security Issues, General Accounting Office, in testimony before the Subcommittee on Cyber Security, Science, and Research and Development and the Subcommittee on Infrastructure and Border Security, Select Committee on Homeland Security, U.S. House of Representatives, Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues, GAO-03-1165T, September 17, 2003, and DHS HITRAC Office during 2006.

Extreme weather routinely affects the sector (e.g., loss of electric power and water during hurricanes, tornados, or earthquakes) and, therefore, nearly all facilities and their workforce personnel have hazard mitigation plans. Weather hazards typically do not rise to the level of a national emergency, but can occasionally threaten regions. According to industry representatives consulted in the preparation of this SSP, weather hazards can be potential vulnerabilities, particularly disruptive to just-in-time delivery practices.

3.5.2 Process for Threat Analysis

HHS will draw upon the sector's infrastructure protection subject matter expertise during the ongoing threat analysis process. During early 2006, HHS shared this analysis with DHS HITRAC to seek comment and to ensure that its 2006 threat assessments are valid.

3.5.3 Specific Threat Information

Specific threat information is critical, infrastructure-specific, and based on real-time intelligence. HHS acknowledges the importance of such intelligence in driving short-term protective measures to mitigate risk. As this intelligence appears, it will also contribute to the general threat environment and common threat scenario products of DHS intelligence bodies, such as HITRAC.

3.6 The Path Forward

In order to address the issues outlined in this section, the sector (GCC, SCC, and all relevant CI/KR protection partners) will need to undertake many tasks as the program matures. The list below addresses some of these. For the specific tasks to be undertaken in the coming year, please refer to the table in section 6.2, Implementation Actions.

3.6.1 Evaluating Candidate CI/KR

- Update the screening method(s) used to identify candidate CI/KR to ensure they meet NIPP annex 4 requirements;
- Review the process and criteria developed over the course of the last 2 years, including an investigation of whether a systems-based approach could be useful in defining what is critical to the sector;
- Review the candidate CI/KR identified in this section to determine if they are appropriate for subsequent examination;
- Develop an updated list of CI/KR for subsequent detailed assessments; and
- Develop improved ways to obtain continuing access to appropriate intelligence streams as a means of assessing threats and vulnerabilities facing the sector.

3.6.2 Developing an Integrated View of Sector Risk/Vulnerability Assessments

- Identify additional vulnerabilities, if any, not identified in prior assessments;
- In partnership with the owners and operators of private and public facilities, assess the vulnerabilities identified in the SSP with a view to refining existing evidence, changes in vulnerabilities, recent experience, and related factors;
- Update the working list of vulnerabilities to which the sector is susceptible;
- Develop a more fully integrated view of the wide range of CI/KR protection-related assessments conducted throughout the Healthcare and Public Health Sector, whether conducted by HHS, other Federal agencies, State authorities, local governments, or private sector bodies;

- Use the results to develop a precise sense of specific CI/KR protection-related risk assessment programs that:
  - HHS, VA, and/or DoD should encourage, modify, or implement to maximize its impact on risk assessments in the sector as a whole; and
  - The private sector should undertake, strengthen, or modify, as appropriate; and
- Assess how vulnerabilities, threats, and consequences identified as particularly relevant to the sector can be integrated into DHS risk management programs.

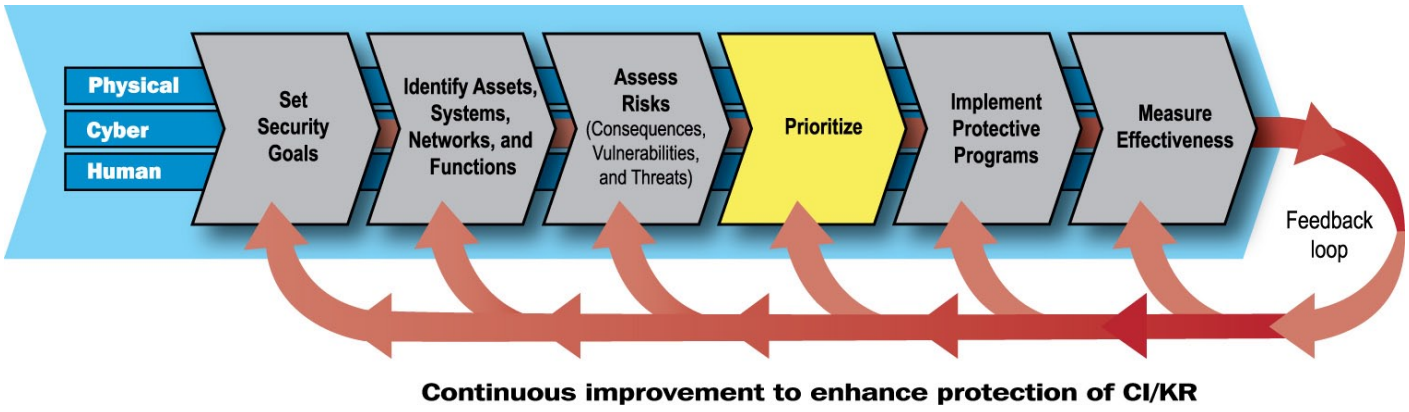
3.6.3 Improving Risk-Reduction Practices

- Continue to examine practices within and across sectors to refine risk management processes;
- By the end of fiscal year (FY) 2007, work to quantify the interdependencies between the Healthcare and Public Health Sector and its other security partners, and bridge the gaps in protecting CI/KR; and
- Develop improved ways to obtain continuing access to appropriate intelligence streams as a means of assessing threats and vulnerabilities facing the sector.

4. Prioritize Infrastructure

The Healthcare and Public Health Sector's CI/KR protective measures are intended to meet several objectives as follows: (1) ensure the broadest support possible across multiple types of disasters; (2) provide resiliency and redundancy in the event that specialized resources are needed simultaneously in multiple regions; (3) reinforce response times during disasters; and (4) mitigate disruption caused by any single point of failure, including those related to human resources, capital, and supplies. These objectives are consistent with the overall risk management framework shown below.

Figure 4-1: Prioritize Infrastructure



While the effectiveness of healthcare and public health operations relies on the capabilities of other sectors, especially water, transportation, and electrical power, this section of the SSP deals only with prioritization of CI/KR within the sector. As required by DHS guidance, the major topic of discussion in this section is the current process for prioritizing sector assets.

4.1 Current Process for Prioritizing Sector Assets

HHS has delegated authority for prioritizing sector assets to ASPR. This important process is proceeding via consultation among representatives of DHS, VA, DoD, the GCC, the SCC, and other stakeholders. Prioritization, moreover, is an iterative process. Its long-term success depends on flexible readjustments in the light of experience, success in developing protective programs, changes in risk environment, improved protective technologies, and other mitigating factors.

4.1.1 Criteria for Prioritization

Risk-based protective programs devote resources where they contribute most to the mitigation of risk. Sector prioritization relies heavily on identifying the roles that each of the sector's CI/KR play in mitigating and responding to the threats identified in section 3.

An initial agreed-upon list of CI/KR is not yet complete, nor has the number of CI/KR been established, although such efforts are underway. For these reasons, the complexity of the process is as yet unknown.

At present, using HITRAC's SHIRA methodology, HHS will prioritize the criticality of assets, systems, functions, and the supporting workforce by assessing each against the HSC and DHS threat scenarios.[53, 54] The SHIRA process provides a methodology for assessing vulnerabilities—recognizability, countermeasure effectiveness, and robustness—against specified threat themes to provide a holistic view of potential consequences. A threat theme is only applied to the extent that it is likely to occur in the sector. The intent is to determine how many scenarios a given asset, system, or capability is relied upon for significant protection, response, or mitigation.

4.1.2 Basis for Prioritization

Once a list of CI/KR is identified for the sector, a preliminary list of criteria created by HHS assists in placing them in rough priority order. These criteria include, but are not necessarily limited to, the following:

- Does the asset perform a function or functions that can have national significance under anticipated threat-related circumstances?
- Are there a small number of such assets performing these function(s) of potential national significance?
- If there is more than one such asset, how widely dispersed geographically (and therefore survivable) are they?
- Is the asset a repository of uniquely valuable expertise largely (or completely) unavailable elsewhere in the country?
- Is the asset crucial in a regional response to one or more nationally significant threats?
- Is the asset crucial in a national response to one or more of these threats?
- Is the asset an important early-warning system for bio-threats?
- Is the impact of destruction or incapacitation of the asset high in terms of the consequences for healthcare and/or public health on a major scale?
- To what extent can the asset be replaced or compensated for in the short term if destroyed or incapacitated?
- If the asset could not be replaced or compensated for in the short term, could the effects on healthcare or public health be catastrophic?
- If an IT asset, what would the effects be if the confidentiality, integrity, and/or availability of the information system were compromised?

Proposed assets, systems, and capabilities will be reassessed in light of ongoing experience. This reassessment will be conducted drawing on the GCC, the SCC, and other resources.

[53] Homeland Security Council, Planning Scenarios Created for Use in National, Federal, State, and Local Homeland Security Preparedness Activities, Version 2.0, July 2004.

[54] DHS, Ranking Guidance for the Strategic Homeland Security Infrastructure Risk Assessment, September 7, 2006.

4.1.3 Frequency of Prioritization Efforts

HHS expects the prioritization process to be repeated each year. In this way, priorities can be adjusted in the light of experience, success in developing protective programs, changes in the threats faced, and other factors. HHS expects that the GCC, the SCC, and other sector partners will continue to play major roles in these reprioritization efforts.

4.1.4 Risk-Based Prioritization Approach

The current prioritization process is not risk-based since risk assessments have not yet been completed for all assets that will be identified using the process just described. The sector intends to use a risk-based prioritization approach as soon as the final list of CI/KR have been identified and risk assessments for these assets can be completed.

4.1.5 Specificity of Prioritization

At present, it appears likely that prioritization will result in several broad bins for CI/KR (e.g., high, medium, and low). These bins will be modified, as needed, based on year-to-year experience.

4.2 The Path Forward

In order to address the issues outlined in this section, the sector (GCC, SCC, and all relevant CI/KR protection partners) will need to undertake many tasks as the program matures. The list below addresses some of these. For the specific tasks to be undertaken in the coming year, refer to the table in section 6.2, Implementation Actions.

4.2.1 Reviewing All Available Results of Prior Steps

- Review all criteria for establishing priorities described in this section;
- Review all risk-oriented assessments made during the prior year in light of experience, additional data, and refinements in the DHS guidance, if any;
- Determine the updates to risk-oriented results needed during the upcoming year; and
- Validate the need for these updates using the GCC, SCC, other authoritative bodies, and appropriate techniques.

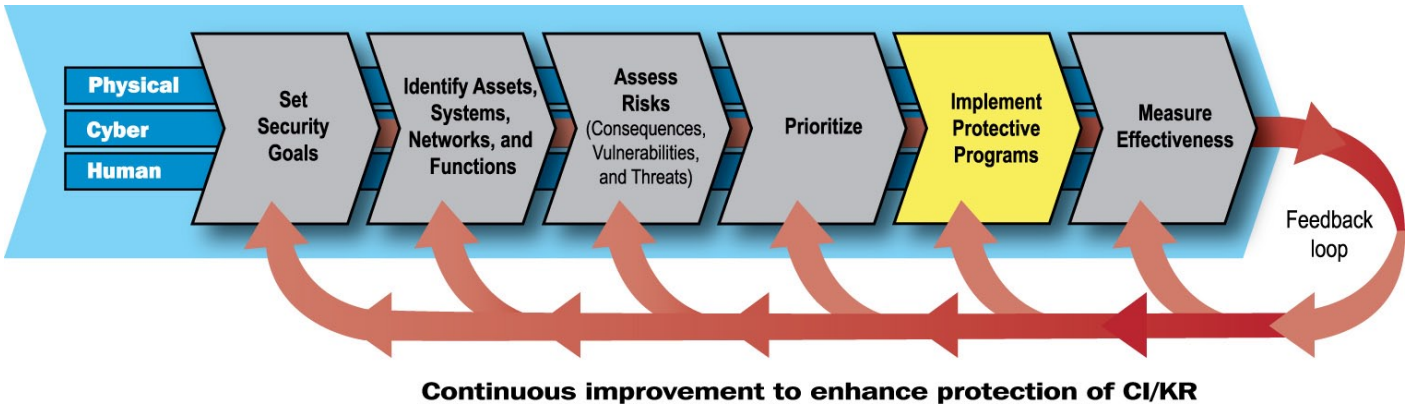
4.2.2 Carrying Out Risk Assessments of Final CI/KR

- Develop a risk-based prioritization approach to sector CI/KR; and
- Carry out the risk analyses of CI/KR identified during prior steps and submit these results to the GCC and SCC for review and comment or approval.

5. Develop and Implement Protective Programs

This section summarizes various major sector security partners' protective programs. It proposes processes to identify, assess, select, and implement protective programs based, in part, on a review of programs already in place. This section is consistent with the DHS risk management framework as shown below.

Figure 5-1: Implement Protective Programs



Major topics in this section include the following:

- Overview of sector protective programs;
- Determining protective program needs;
- Protective program implementation;
- Protective program performance; and
- The path forward.

5.1 Overview of Sector Protective Programs

Like other SSAs, HHS is not solely responsible for development and implementation of protective programs across the sector. It does, however, facilitate the effective implementation of protective programs by coordinating with its public, private, and other security partners. The overall intent of protective programs is to manage risk by deterring threats, mitigating vulnerabilities, and/or minimizing consequences. The most effective protective programs are comprehensive, coordinated, cost-effective, risk-based, consistent with established programs, and sensitive to cultural differences among any affected parties.

5.1.1 Protective Program Landscape

Protective programs vary from one entity to another. These programs have been developed by government and private sector security partners. Each responds to its own mandates and imperatives, many pre-dating HSPD-7. The Healthcare and Public Health Sector fulfills a response and recovery support role serving all other sectors in times of manmade or natural disasters. As a result, the sector tends to place great importance on protective programs that emphasize post-incident response activities or plans that enable a return to normal status. However, all protective programs generally include steps focused on deterrence, defense, damage limitation, and reconstitution. The desired outcomes of protective programs include, but are not limited to, prevention of mass casualties, assurance of the continued functioning of the economy, avoidance of cascading disruptions, and maintenance of public confidence.

These programs address a wide range of measures that relate to the sector's goals of protecting physical structures and the ability to deliver care, as well as ensuring the security of IT assets and the sector's workforce. Although these activities may not be totally integrated, they do work together to protect the sector; for example, when looking at hospital facilities, private programs at the hospital level work in concert with State and local regulations. In addition, the accreditation process most hospitals go through with the Joint Commission for the Accreditation of Healthcare Organizations ensures that the sites meet minimum criteria for physical, cyber, and workforce security, in addition to other measures, and are audited periodically to maintain their accreditation. From the Federal level, the hospitals are the recipients of funding through CDC and Health Resources and Services Administration (HRSA) grants and cooperative agreements. The awarding of these funds is coordinated with (and sometimes the funds flow through) the State and local governments, and the funds are targeted based on needs identified through a collaborative process. HHS is actively working to ensure that CI/KR protection concerns continue to be integrated into the guidance for these programs.

Another example of how protective programs fit together pertains to the protection of critical assets identified response planning. Certain manufacturers of key pharmaceuticals and supplies undertake their own protective measures based on their business interests. In addition, regulatory guidance from Federal (e.g., FDA) and State authorities requires that protective programs be in place at facilities. Once identified as a nationally critical asset, a facility may be approached by HHS and the DHS and asked to allow the Federal Government to conduct a site visit, in concert with local law enforcement, to make suggestions regarding protective measures in all areas (physical, cyber, and workforce). In addition, through the Buffer Zone Protection Program (BZPP), State and local governments may receive Federal funding targeted at protecting the nationally critical facility.

Table 5-1 describes several of the sector's protective programs and relates them to the sector's goals of protecting physical, cyber, and workforce elements. Among other things, this description shows the variety of organizations and mandates involved. Because of the sector's diversity and its risk impacts, a variety of protective programs exist; however, as the examples above suggest, they complement each other to protect the sector. For more information on all of these programs and many more, refer to appendix 5.

Table 5-1: Sector Protection Efforts Aligned With Sector Security Goals

	Sector Protective Programs and CI/KR Protection Efforts	Description
Physical Security		
Department of Homeland Security Programs	Buffer Zone Protection Program	BZPP is designed to reduce the vulnerabilities of CI/KR sites by extending the protected area around a site into the surrounding community and supporting prevention and preparedness efforts.
Health and Human Services Programs	HHS agency physical security program	Provides the appropriate policies, procedures, and technologies to ensure that a high-level security posture is maintained throughout organizational offices, laboratories, storage areas, utilities, and support systems.
	Joint HRSA/DHS Site Visits	Assesses approximately 10 private sector hospitals per year in connection with the Bioterrorism Hospital Preparedness Program.
Department of Veterans Affairs	VA Office of Cyber and Information Security, Review and Inspection Division	Has primary responsibility for conducting yearly assessments of the physical security of representative VA facilities.
	VA Office of Facilities Management in coordination with the Offices of Security and Law Enforcement	Physical Security Site Assessments Program: Assesses VA facilities and critical infrastructures in compliance with National Security Policy Directives, Presidential Decision Directives (PDDs), and legislation.
	VA Emergency Preparedness Assessment Tool	Conducts analysis of facility and staff preparedness in areas such as medical center backup utilities, laboratory and pharmacy facilities, psychiatric services, security, administration, and internal medicine.
Department of Defense	DoD Health Affairs	Has overall responsibility for the DoD healthcare CI/KR protection issues, including identifying critical assets, conducting vulnerability assessments, and taking mitigating actions to provide mission assurance.
Private Sector Programs	ASIS Pharmaceutical Security Council	Promotes security leadership and cooperation between all segments of the pharmaceutical industry and acts as an industry resource for everything from business continuity and risk assessments to cyber preparedness and insider threat.
	Pharmaceutical Security Institute (PSI)	A non-profit group whose mission is to protect the public health, through the disruption and dismantling of criminal groups involved in counterfeit pharmaceuticals.
Public/Private	InfraGard	Information-sharing and analysis effort serving the CI/KR protection interests; an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

	Sector Protective Programs and CI/KR Protection Efforts	Description
Cyber		
Department of Health and Human Services	Agency Certification and Accreditation Program (FISMA requirement)	Program establishes the thresholds for risk acceptance; identifies system vulnerabilities and mitigation strategies; and ensures the confidentiality, availability and integrity of agency data.
	HHS Personnel Security	Defines the appropriate policies and procedures to assess an individual's (i.e., contractors, vendors, visitors, and all personnel) suitability to access HHS resources and information/information systems.
	Incident response – Secure One Communication Center (SOCC)	Centralizes the HHS cyber incident reporting capability. The SOCC ensures collaboration among all HHS divisions, the Office of the Inspector General, and the United States Computer Emergency Readiness Team (US-CERT).
Department of Veterans Affairs	VA Office of Cyber and Information Security	Manages the Critical Infrastructure Protection Program, has overarching responsibility for assessing, mitigating, and defending against cyber security threats, including those facing the veterans health system.
	VA Agency-Wide IT Information Security Program	Establishes policies, procedures, and guidelines to reduce risk; ensures that security is integrated into the information system life cycle; confirms compliance with applicable statutes and directives; develops security plans; and provides department-wide cyber security awareness training.
Department of Defense	DoD Health Affairs	Has overall responsibility for the DoD healthcare CI/KR protection issues, including identifying critical assets, conducting vulnerability assessments, and taking mitigating actions to provide mission assurance.
Private Sector Programs	ASIS Pharmaceutical Security Council	Promotes security leadership and cooperation between all segments of the pharmaceutical industry and acts as an industry resource for everything from business continuity and risk assessments to cyber preparedness and insider threat.
	PSI	A non-profit group whose mission is to protect the public health, through the disruption and dismantling of criminal groups involved in counterfeit pharmaceuticals.
Public/Private	InfraGard	Information-sharing and analysis effort serving the CI/KR protection interests; an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

	Sector Protective Programs and CI/KR Protection Efforts	Description
Workforce Security		
Department of Health and Human Services	HHS Personnel Security	Defines the appropriate policies and procedures to assess an individual's (i.e., contractors, vendors, visitors, and all workforce personnel) suitability to access HHS resources and information.
	HHS Office of Preparedness and Emergency Operations (OPEO)	Responds to bioterrorism, public health, and medical threats and emergencies, and CI/KR protection efforts.
	Joint HRSA/DHS Site Visits	Assessment of approximately 10 private sector hospitals per year over the past 2 years in coordination with the Bioterrorism Hospital Preparedness Program.
	International Early Warning Surveillance Program	Integral in U.S. Government efforts in surveillance and detection of disease outbreaks overseas.
	Border States Initiatives	Provides cross-border early warning of infectious diseases.
	BioWatch	Detects the release of pathogens into the air, warning the government and public health community in the event of a potential bioterror event.
	Biosurveillance Initiative	Initiative increases the number of quarantine stations at major ports of entry and extends BioSense, CDC's near-real-time human health surveillance system.
Department of Veterans Affairs	VA Emergency Preparedness Assessment Tool	Conducts analysis of facility and staff preparedness in areas such as medical center backup utilities, laboratory and pharmacy facilities, psychiatric services, security, administration, and internal medicine.
Department of Defense	Armed Forces Medical Intelligence Center (AFMIC)	Focal point for compiling all-source intelligence to include the health status of foreign military forces, infectious disease and environmental health risks, and scientific and technical developments in biotechnology and biomedical subjects of military importance.
Department of Labor	Occupational Safety and Health Administration	Aims to ensure worker safety and health by working with employers and employees to create safe, environmentally sound, healthy working environments.
Private Sector	Joint Commission on the Accreditation of Healthcare Organizations (JCAHO)	Promotes effective protective programs using state-of-the-art standards that focus on improving the quality and safety of care provided by healthcare organizations.
	National Committee for Quality Assurance	Evaluates managed care plans for patient safety, confidentiality, consumer protection, and continuous improvement.
	American Society for Information Science (ASIS) Pharmaceutical Security Council	Promotes security leadership and cooperation between all segments of the pharmaceutical industry and acts as an industry resource for everything from business continuity and risk assessments to cyber preparedness and insider threat.
	PSI	A non-profit group whose mission is to protect the public health, through the disruption and dismantling of criminal groups involved in counterfeit pharmaceuticals.
Public/Private	InfraGard	Information-sharing and analysis effort serving the CI/KR protection interests; an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

5.1.2 Recent Legislation Affecting Protective Efforts Across Sectors

In addition to the legislative requirements imposed by homeland security legislation, there are significant Federal statutes, regulatory programs, and security requirements facing nearly all sectors. Many have had a broad impact on the establishment of protective programs and some ensure uniformity of protective program requirements across the sector. Examples of other legislation that have CI/KR protection-related impacts with respect to matters of healthcare and public health are listed below and are also referenced, where appropriate, in table 5-1:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes requirements for, among other things, the privacy and security of individually identifiable health information;
- Public Health Threats and Emergencies Act of 2000 (PHTEA) authorizes the Secretary of HHS to, among other things, take appropriate actions in the event of an infectious disease outbreak or bioterrorism attack;
- Critical Infrastructure Protection Act of 2001 (CIPA) (Title III, Section 1016 of the USA PATRIOT Act of 2001) requires all Federal agencies to take certain steps to protect critical infrastructures under their control;
- Cyber Security Enhancement Act of 2002 (CSEA) (Title II, Section 225 of the Homeland Security Act of 2002) requires all Federal agencies to take certain steps to protect automated IT systems under their control; and
- Federal Information Security Management Act (FISMA) (Title III of the E-Government Act of 2002) requires that Federal agencies provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, including those provided or managed by another agency, contractor, or other source.

5.2 Determining Protective Program Needs

Protective programs must meet a legitimate need in order to be considered for implementation. Such programs should be implemented based on their particular characteristics, as well as the needs of the sector. Cost-benefit analyses should be performed to help the sector prioritize implementation and the need to close gaps. The process for identifying and validating specific protective program needs entails the following sub-processes:

- Identification of needs;
- Development of tools to catalog needs;
- Validation of needs and their specific characteristics; and
- Determination of a basis for including or excluding specific needs from protective programs.

In consultation with its security partners, HHS plans to promote discussions about ways to deal with the following topics:

- Processes to decide whether a gap must be minimized;
- Processes to determine whether closing a gap is possible;
- Thresholds for action;
- Processes to determine what, if any, protective program should be put in place when a gap is identified;
- Processes to balance the costs of implementation against the risk of not addressing the gap;
- Evaluation of existing programs that could potentially be used to close the gap;

- Existing regulations and standards that might aid or inhibit the implementation of a given protective program;
- Processes to develop a new program in the absence of an existing protective program; and
- The extent to which various sector elements will be involved in the selection and implementation of the protective program.

5.3 Protective Program Implementation

The sector is beginning to address implementation and maintenance of protective programs once they are prioritized. During the upcoming year, HHS plans to sponsor discussions on program implementation in consultation with its security partners through the GCC and the SCC. These bodies will serve as forums for discussion and coordination of the following topics:

- Identification of security partners responsible for and involved in protective program development, implementation, and execution;
- Processes to determine security partner input that should be incorporated into or considered in the SSA's protective programs;
- Process for coordinating sector-specific actions with actions already taken by DHS and other security partners;
- Protective program coordination with DHS, other Federal departments and agencies, and State and local governments, as appropriate (e.g., working with DHS's National Cyber Security Division (NCSD) to facilitate cross-sector cyber coordination);
- Roles and responsibilities of the various security partners (e.g., DHS; HHS; owners and operators; other Federal, State, and local entities; trade associations; and academia);
- Process to coordinate with other sectors and with DHS to implement protective actions across sectors that are required to mitigate dependencies; and
- Obstacles that inhibit coordination of sector protective programs and ways to address such challenges.

As appropriate, HHS, DoD, and VA will begin to work more closely with DHS's NCSD, and with US-CERT.

5.4 Protective Program Performance

During the upcoming year, HHS plans to begin addressing the performance of protective programs. Monitoring will be conducted to help determine whether the programs are effective, whether they have closed the gaps they were intended to address, and whether they can be improved. This effort will be directed toward determining the following:

- Process to determine which protective programs are successful and merit continued support;
- Process to evaluate a protective program's effectiveness in relationship to its goals;
- Strategy for improving the sector's processes and mechanisms for communicating successes and recommendations;
- Process to monitor technological developments that might improve or modify protective programs; and
- Process to ensure that future decision-making will utilize information gained from protective program performance monitoring.

Section 6 discusses progress metrics that focus on protective program performance.

5.5 The Path Forward

In order to address the issues outlined in this section, the sector (GCC, SCC, and all relevant CI/KR protection partners) will need to undertake many tasks as the program matures. The list below addresses some of these. For the specific tasks to be undertaken in the coming year, refer to the table in Section 6.2, Implementation Actions.

5.5.1 Developing Plans for Protective Programs

Develop a more complete plan for determining protective program needs including, but not limited to, the following:

- Surveying existing protective programs to identify major gaps that may exist relative to CI/KR;
- Investigating cost-effective ways to fill these gaps or reduce their significance;
- Developing a strategy for promoting the necessary gap-filling programs;
- Identifying funding sources for these programs; and
- Identifying near-term assessment possibilities.

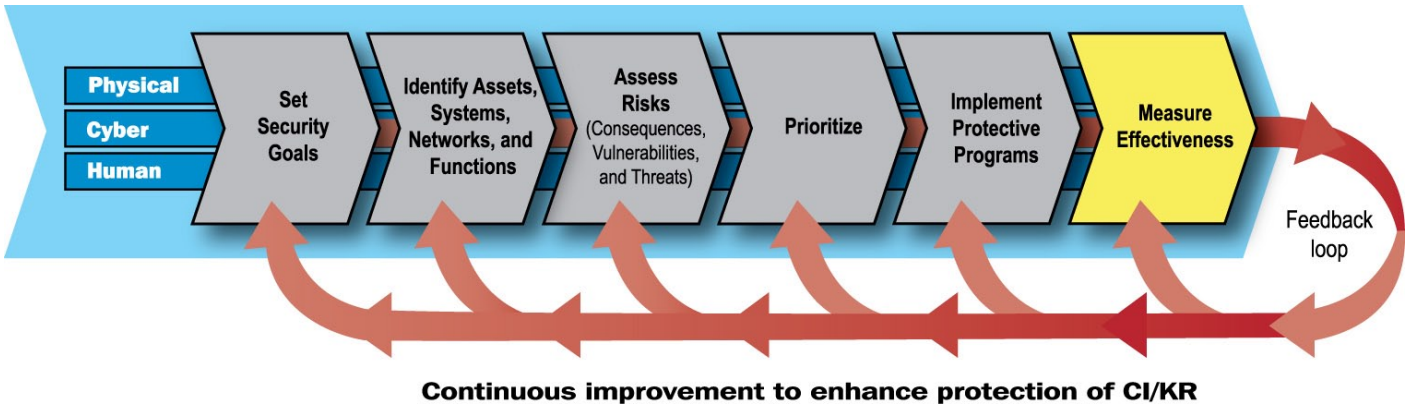
5.5.2 Developing Processes for Protective Program Development

- Establish appropriate working groups to deal with the issues raised by the SSP in connection with protective program needs and program development; and
- Identify a process for coordinating with other relevant sectors to implement cross-sector protective programs, as appropriate.

6. Measure Progress

Measuring progress is a fundamental aspect of the NIPP risk management framework and appropriate metrics must be employed to measuring sector progress made by the sector toward CI and KR protection goals. HHS has been working with the DHS Metrics Working Group to formulate standards, processes, and ultimately NIPP Metrics Guidance to ensure consistency in measuring progress. These metrics are both qualitative and quantitative. They can provide focus to improve the effectiveness of the tasks at hand, supporting budget requirements, a change in program direction, and the establishment of new processes or additional resources. Performance measures can be a very powerful tool if leveraged correctly.

Figure 6-1: Measure Effectiveness



Major topics in this section include the following:

- CI/KR performance measurement;
- Implementation actions;
- Challenges and continuous improvement; and
- The path forward.

6.1 CI/KR Performance Measurement

DHS will develop core metrics that are designed to apply across all CI/KR assets and allow for comparison between sectors. Each sector, in turn, develops sector-specific metrics intended to focus on the unique characteristics of that sector. Three kinds of metrics are under consideration in the Healthcare and Public Health Sector. Consistent with Section 3.6 of the NIPP, they include the following:

- Descriptive metrics that focus on sector resources and activities;
- Process metrics that focus on the output of a process or track the progression of a particular task; and
- Outcome metrics that focus on progress toward achievement of a strategic CI/KR protection goal.

Examples of all three types of metrics appear in tables 6-1 through 6-6. These serve as a basis for discussion among the GCC and SCC membership. This discussion will include, but not necessarily be limited to, the consistency of these metrics with applicable national guidance. They should also be assessed (and modified as needed) in terms of their feasibility. In tables 6-1 through 6-6, each draft metric is described in terms of four characteristics:

- Types and examples of metrics;
- Preliminary description;
- How it will be assessed; and
- The authorities likely to be responsible for the assessment.

6.1.1 Developing Sector-Specific Draft Metrics

The example metrics shown in tables 6-1 through 6-6 were reviewed in 2006 by public and private sector representatives. They have also been vetted with all relevant authorities and with the GCC and the SCC. It is anticipated that these metrics will be refined in 2007 and that additional metrics may be added based on recommendations from GCC/SCC work groups and based on common key performance indicators utilized throughout the sector in the measurement of risk management programs.

Initially, performance indicators will cover a combination of descriptive, process, and outcome measures, providing a balanced context for improvement to CI/KR protection efforts. Continuous improvement may require a re-prioritization of CI/KR assets, an adjustment in security goals, or additional outputs to protective programs. It will also be necessary during this process to assess measures for accuracy, relevance, and whether they are actionable. As the SSP goes through implementation, process metrics and descriptive metrics will give way to outcome metrics, enabling a more holistic, strategic view of sector progress.

It is anticipated that separate sector-specific measures for cyber security will be created through work group sessions and surveys. Once DHS finalizes core cyber measures, the sector will review sector-specific measures for gaps between the two components. Brainstorming and collaboration will be necessary throughout this process in order to ensure that all participants understand what is being measured, how it is being calculated, and what their role is in the measurement. In addition to this, close coordination DHS National Cyber Security Division (NCSD) and other security partners will provide the sector with a venue for validating cyber security measures.

6.1.2 Information Collection and Verification

Collecting data that support these metrics in all appropriate sectors is a challenging task. It may take months to collect requirements, standardize definitions, prioritize and verify metrics, and solicit feedback, and the metric could fail. Issues of feasibility, validity, reliability, currency, and cost are significant. Metrics must be implemented, reviewed, and then adjusted based on how they impact performance or behavior.

In order to promote performance goals that are consistent with the overall entity goals, the sector will solicit input from all parties to collect and document entity goals. These goals can then be mapped to CI/KR protection goals to validate that they are actionable, consistent, and aligned. This increases the likelihood that both will be achieved. Other topics that will be determined through collaboration and work group sessions include the following:

- Parties that should be responsible for data collection—some parties have been identified in tables 6-1 through 6-6; however, these need to be validated;
- Methods for data collection (e.g., by on-site survey, mail survey, statistical sample) that are feasible within practical, regulatory, and other constraints. If surveys are to be used, the process for creating a survey, requirements for anonymity, resource requirements, analysis, and reporting processes, etc., will need to be developed;
- Methods for assuring that metrics-related information will be capable of both aggregation and dis-aggregation as needed;
- Whether sensitive or proprietary information will be collected;
- If sensitive or proprietary information is to be collected, how it will be protected;
- Verification that the information collected is accurate and identification of the party or parties that will perform the verification (e.g., the SSA, a contractor, some other third party);
- Methods for scoring and rating the results of applying the metrics. We anticipate that DHS technical assistance sessions for developing metrics may elaborate on best practices for scoring and rating results; and
- Methods for assuring that performance measure data are updated appropriately.

The sector collected information during 2006 as part of the metrics and annual reporting process and will continue to address this set of tasks in 2007.

Table 6-1: Descriptive, Process, and Outcome Metrics for Facilities and Systems (Federal, State, Local, County, Tribal, and Private)

Type and Examples of Metrics	Preliminary Description	How Assessed	Assessment Authorities Responsible
Descriptive			
Percentage of total assets characterized in CI/KR terms by class	Review of healthcare and public health facilities and systems managed by Federal, State, County, Local, Tribal, and private sector agencies	Review of data using approved methods	Relevant staff with CI/KR responsibilities
Number of assets with potential for medium or high consequences if damaged or destroyed	Review of healthcare and public health facilities and systems managed by Federal, State, county, local, tribal, and private sector agencies	Review data using approved methods	Relevant staff with CI/KR responsibilities

Type and Examples of Metrics	Preliminary Description	How Assessed	Assessment Authorities Responsible
Process			
Percentage of high-consequence assets rated as high risk using validated methods	Review of healthcare and public health facilities and systems managed by Federal, State, county, local, tribal, and private sector agencies	Rating of facilities and systems using approved methods	Relevant staff with CI/KR responsibilities
Percentage of key staff aware of need for protective programs tailored to the threats their facility faces	Review of healthcare and public health facilities and systems managed by Federal, State, county, local, tribal, and private sector agencies	Use of appropriate survey and interview results	Relevant staff with CI/KR responsibilities
Outcome			
Percentage of risk and vulnerability assessments completed	Validation and approval of risk and vulnerability assessments completed	Assessments using approved methods	Relevant staff with CI/KR responsibilities
Percentage of high-consequence assets with defined, approved, cost-effective protective programs	Validation of healthcare and public health facility protective plans	Assessments using approved methods	Relevant staff with CI/KR responsibilities
Percentage of high-consequence assets with audited plans	Evaluation of validation results	Assessments using approved methods	Relevant staff with CI/KR responsibilities
Percentage of security key staff who have completed CI/KR protection training programs	Evaluation of the degree to which security officers have received updated training in CI/KR protection issues	Assessments using approved methods	Relevant staff with CI/KR responsibilities
Percentage of assets lowered from high risk to a lower risk category	Comparison of "before" and "after" evaluation of validation results	Comparison using approved methods	Relevant staff with CI/KR responsibilities

Table 6-2: Descriptive, Process, and Outcome Metrics for the Federal Workforce

Type and Examples of Metrics	Preliminary Description	How Assessed	Assessment Authorities Responsible
Descriptive			
Percentage of total workforce assets characterized in CI/KR terms by class	Review of healthcare and public workforces managed by Federal, State, county, local, tribal, and private sector agencies	Review of data using approved methods	Relevant staff with CI/KR responsibilities
Workforces with potential for medium or high consequences if incapacitated	Review of healthcare and public workforces managed by Federal, State, county, local, tribal, and private sector agencies	Review of data using approved methods	Relevant staff with CI/KR responsibilities

Type and Examples of Metrics	Preliminary Description	How Assessed	Assessment Authorities Responsible
Process			
Percent of high-consequence workforce assets rated as high risk using validated methods	Rating of healthcare and public health workforces managed by Federal, State, county, local, tribal, and private sector agencies	Rating of workforces using approved methods	Relevant staff with CI/KR responsibilities
Percent of key staff aware of need for protective programs tailored to the threats their workforces face	Rating of healthcare and public health workforces managed by Federal, State, county, local, tribal, and private sector agencies	Rating of workforces using approved methods	Relevant staff with CI/KR responsibilities
Outcome			
Percent of high-consequence workforces covered by defined, approved, cost-effective protective programs	Validation of healthcare and public health workforce protective plans developed by Federal, State, county, local, tribal, and private sector agencies	Assessments using approved methods	Relevant staff with CI/KR responsibilities
Percent of high-consequence workforces with audited plans	Evaluation of validation results	Assessments using approved methods	Relevant officials at HHS, VA, and DoD with CI/KR responsibilities
Percent of workforces lowered from high risk to a lower risk category	Comparison of "before" and "after" evaluation of validation results	Comparisons using approved methods	Relevant staff with CI/KR responsibilities

6.1.3 Reporting

HSPD-7 requires each SSA to report annually to the Secretary of Homeland Security on progress in the implementation of CI/KR protection programs.[55] Within HHS, this responsibility is carried out by ASPR. The annual reports to be developed under this task for DHS will accomplish, but not necessarily be limited to, the following:

- Provide a common vehicle across all CI/KR sectors to communicate CI/KR protection priorities and progress to security partners and other government entities;
- Establish a baseline of existing sector-specific CI/KR protection programs and initiatives;
- Identify plans for SSA resource requirements and the departmental CI/KR protection budget;
- Describe how sector efforts support the national effort;
- Provide an overall CI/KR protection progress report for the sector;
- Measure that progress toward sector CI/KR protection goals against the national protection goals for that sector;
- Provide feedback to DHS, sector security partners, and other government entities that will be used as a basis for the continuous improvement of the CI/KR protection program; and

[55] See HSPD-7, Paragraphs 27 and 35.

• Help identify and share best practices from successful CI/KR protection programs.

During 2006, HHS submitted the Sector CI/KR Protection Annual Report (Sector Annual Report) to DHS. This submission documented sector activities and included the HHS submission to the NIPP metrics process. During 2007, HHS will again submit its annual report and will continue to refine the submission to more accurately and completely reflect sector status and progress.

6.2 Implementation Actions

"The Path Forward" at the end of each section lays out a broad range of activities that must be addressed in order to implement a complete program. Table 6-7 describes the tasks that the sector will focus on in 2007.

Table 6-3: Implementation Actions as Defined in the National Infrastructure Protection Plan

X = Primary responsibility O = Support responsibility

\+ = Milestone indicator NLT = Not Later Than

Implementation Actions	Milestone					Security Partner			
	NLT 90 Days After SSP Release	NLT 180 Days	NLT 365 Days	Specific Date	DHS	SSA	Other Federal Agencies	State, Territory, Locality, Tribe	Private Sector
Sector Profile and Goals									
Review and refine sector security mission, vision, goals, and objectives.			+		X	X	X	X	X
Refine the sector profile.			+			X			
Establish relationships with SSAs, SCC, and GCC for sectors that are dependent, interdependent, or overlapping with the Healthcare and Public Health Sector.			+		X	X			
Define international partners and investigate international interdependencies.		+			X	X	X		X
Identify Assets, Systems, Networks, and Functions									
Refine the NADB taxonomy for sector infrastructure.		+			X	O	O	O	O
With sector security partners, develop a plan for CI/KR protection-related data collection within the sector.		+			X	X	O	O	O
Assess Risks (Consequence, Vulnerabilities, Threats)									
Review existing risk assessment methodologies to determine compatibility with the NIPP baseline criteria.		+			O	X	O	O	O
Establish timeline for the development of sector-specific risk methodologies.		+			X	X			

X = Primary responsibility O = Support responsibility

\+ = Milestone indicator NLT = Not Later Than

Implementation Actions	Milestone					Security Partner			
	NLT 90 Days After SSP Release	NLT 180 Days	NLT 365 Days	Specific Date	DHS	SSA	Other Federal Agencies	State, Territory, Locality, Tribe	Private Sector
Form a security partner team to develop criteria for defining critical assets.		+				X	O	O	O
Establish a timeline for conducting consequence-based top-screening for all sector infrastructure.		+			O	X	O	O	X
Initiate performance of consequence-based top-screen for sector infrastructure.			+		O	X	O	O	O
Conduct and validate consequence assessments of priority CI/KR as identified by the top-screening process.			+		O	X	X	O	O
Develop sector-specific CI/KR threat assessments needed to support comprehensive risk assessments.	+				O	X	O	O	O
Prioritize Infrastructure									
Review and refine the process for prioritizing sector infrastructure.			+		O	X			
Conduct or facilitate vulnerability assessments of priority CI/KR and identify common vulnerabilities.			+		X	O X	X	X	X
Develop and Implement Protective Programs									
Establish a security partner team to begin development of a coordinated, sector-wide protective program.		+			X	X	O	O	O
Determine highest priority protective program needs/gaps and identify potential solutions to remedy those gaps.			+		O	X	X	O	O
Incorporate CI/KR and security partners into national exercises.			+		O	X	O	O	O
Measure Progress									
Form a security partner team to address sector-specific metrics.		+				X			
Develop sector-specific metrics.			+			X	O	O	O

X = Primary responsibility O = Support responsibility

+ = Milestone indicator NLT = Not Later Than

Implementation Actions	Milestone					Security Partner			
	NLT 90 Days After SSP Release	NLT 180 Days	NLT 365 Days	Specific Date	DHS	SSA	Other Federal Agencies	State, Territory, Locality, Tribe	Private Sector
CI/KR Protection Research & Development									
Form the sector's CI/KR protection R&D Governance Organization.			+			X	X	O	O
Develop and communicate requirements for CI/KR-related R&D to the DHS for use in the national R&D planning effort.				July 1 annually		X	X		X
Managing and Coordinating SSA Responsibilities									
Form a security partner team to address issues related to information sharing.		+			X	X	O	O	
In collaboration with the security partner team, develop suggested information-sharing processes for the sector.			+			X	X	X	X
Develop and roll out HSIN-Critical Sector (HSIN-CS) for the Healthcare and Public Health Sector.			+		X	X			
Implement a PCII program at HHS and in the sector.			+			X			
Develop and submit Sector CI/KR Protection Annual Report.				July 1 annually	O	X	O	O	O

6.3 Challenges and Continuous Improvement

As figure 6-1 indicates, metrics play a key role in prompting steady improvement in the protection of sector assets. Progress in one year leads to steps for improvement in the next. The example metrics summarized in tables 6-1 through 6-6 were reviewed and commented upon by public and private sector representatives during 2006. All comments and suggestions have been adjudicated and adopted as warranted. The next step, as indicated in previous sections, is to obtain the review and comments of the GCC, the SCC, and other appropriate authorities on performance metrics. In addition, further work by the DHS NIPP metrics group will be incorporated. These efforts will be accompanied by the development of a plan for implementing a more robust process for measuring progress, once CI/KRs have been appropriately identified prioritized, assessed, and protected.

In order that metrics will be used to guide future decisions, the sector needs to determine:

- Procedures for incorporating metrics into the decision-making process;
- How metrics will be used to measure progress toward goals;

- The process for determining whether metrics indicate that sector activities are on track;
- The process for addressing insufficient progress toward identified goals; and
- Challenges in developing and using metrics and plans to address these challenges (e.g., challenges presented by voluntary participation in protective program implementation).

6.4 The Path Forward

In order to address the issues outlined in this section, the sector (GCC, SCC, and all relevant CI/KR protection partners) will need to undertake many tasks as the program matures. The list below addresses some of these. For the specific tasks to be undertaken in the coming year, refer to the table in section 6.2, Implementation Actions.

6.4.1 Improve Progress Metrics

Steps in refining and vetting progress metrics include the following:

- Circulate draft metrics among appropriate representatives from each affected Cabinet-level Federal agency with healthcare and public health responsibilities (e.g., HHS, VA, DoD) for review and comment;
- Circulate draft metrics among appropriate representatives of the private sector with healthcare and public health responsibilities;
- Circulate draft metrics among appropriate representatives of affected State, county, tribal, and city public health agencies and laboratories;
- Convene a formal working group to consolidate and refine comments received from these strategic partners;
- Review the above results to verify that the combined list of metrics meets all applicable requirements and guidance; and
- Review the above results to verify that the necessary metrics can be collected, scored, and that ratings can be derived.

6.4.2 Plan Implementation Actions

Steps in implementation planning should include the following:

- Establish a joint GCC/SCC committee to assist HHS in planning the implementation steps outlined in DHS guidance;
- Develop recommendations for review and approval by HHS in consultation with DHS;
- Formulate a plan for executing the recommendations approved by HHS in consultation with DHS; and
- Formulate a plan for testing the usefulness of metrics in assessing the ability of an asset to respond to various threat scenarios and/or real events for which appropriate data exist.

7. Planning Healthcare and Public Health Sector CI/KR Protection R&D

This section of the SSP focuses on R&D efforts to improve the protection of sector CI/KR during the coming year. This sector, like nearly all others in the United States, needs new technologies to assist in the protection of major assets. Improved technologies can help preserve and strengthen the sector's ability to meet the Nation's needs in emergency and non-emergency circumstances alike. Moreover, many sectors have similar needs for protective R&D. If R&D efforts are shared appropriately, they can meet these needs in the most cost-effective manner possible. Major topics in this section include the following:

- Overview of sector R&D;
- Sector R&D requirements;
- Sector R&D plan;
- R&D management processes; and
- The path forward.

7.1 Overview of Sector R&D

Federal CI/KR protection R&D planning is based on HSPD-7, which states that:

> *"In coordination with the Director of the Office of Science and Technology Policy, the Secretary (of DHS) shall prepare on an annual basis a Federal Research and Development Plan in support of this Directive."*[56]

This overall objective is buttressed by planning at the national level in the form of The National Plan for Research and Development in Support of Critical Infrastructure Protection (NCIP R&D Plan).[57]

7.1.1 Strategic Goals

As a component of the NIPP, the NCIP R&D Plan has three strategic goals. Intended to help ensure the future security of the Nation's critical infrastructure, these goals are the following:[58]

[56] See Executive Office of the President, HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, paragraph 30, December 17, 2003.

[57] See Executive Office of the President, Office of Science and Technology, and DHS, Science and Technology Directorate, *The National Plan for Research and Development in Support of Critical Infrastructure Protection,* April 8, 2005, www.dhs.gov/interweb/assetlibrary/ST_2004_NCIP_RD_PlanFINALApr05.pdf.

[58] Topics covered by these ancillary plans include, but are not limited to, R&D plans oriented toward radiological/nuclear countermeasures; law enforcement; social, behavioral, and economics factors; biological countermeasures; chemical countermeasures; cyber countermeasures; intelligence; standards; and emergency preparedness and response.

- Achieving a national common operating picture for critical infrastructure;
- Promoting a next-generation computing and communications network with security "designed in" and inherent in all elements rather than added after the fact; and
- Encouraging resilient, self-diagnosing, and self-healing physical and cyber infrastructure systems.[59]

7.1.2 Overall Themes

Consistent with these goals, the NCIP R&D Plan is structured around nine science, engineering, and technology themes. These themes apply in all sectors; encompass physical, cyber, and workforce concerns; and are integrated into a layered security strategy for protecting all CI and KR.[60]

Each of these themes applies across all sectors of the U.S. economy.[61] Each is beneficial to both public sector and private sector entities. Each addresses short-, middle-, and long-term CI/KR protection needs. Each must draw on natural, applied, and social sciences in addition to anecdotal evidence to achieve the desired results.

7.1.3 R&D Research Priorities

Consistent with these themes, eight CI/KR protection-related research priorities are identified in the NCIP R&D Plan.[62] Under the leadership of the White House Office of Science and Technology Policy (OSTP), a combined CI/KR protection R&D program drawing on relevant Federal agencies should develop an integrated national CI/KR protection R&D program. This program should fill important gaps in R&D research relevant to CI/KR protection, but minimize unnecessary overlaps and redundancies in these programs across Federal agencies. DHS has sponsored initial Federal Government-wide discussions of overall Federal R&D in this area, and these discussions continue. A review of privately sponsored academic research is warranted as well.

7.1.4 Healthcare and Public Health Sector R&D Status and Goals

As in other sectors, planning for CI/KR protection R&D must take into account the Federal, State, county, local, and tribal levels, as well as the private sector requirements. The current status of each is summarized below.

CI/KR Protection R&D at the Federal Level. The three Federal departments with significant healthcare and public health responsibilities—HHS, VA, and DoD—all have robust R&D agendas. Collectively, they focus on relevant legislative mandates acquired over each department's history. Historically, these R&D programs have been based on mission-focused goals that did not necessarily emphasize CI/KR protection.

To fulfill the applicable requirements of HSPD-7, the R&D programs of all three Cabinet-level departments are being reviewed to identify R&D programs with CI/KR protection significance. In addition, other unrelated Federal agencies conduct R&D that can benefit the Healthcare and Public Health Sector. These R&D programs are being reviewed as well. In this way, an integrated view of Federal Government-wide R&D of potential value in protecting sector-critical assets can be developed.

[59] See Executive Office of the President, Office of Science and Technology Policy, and DHS Science and Technology Directorate, The National Plan for Research and Development in Support of Critical Infrastructure Protection, Executive Summary, p. vi.

[60] These themes include detection and sensor systems; protection and prevention; entry and access portals; insider threats; analysis and decision support systems; response, recovery, and reconstitution; new and emerging threats and vulnerabilities; advanced infrastructure architectures and systems design; and human and social issues.

[61] They also correspond in a rough manner to the homeland security mission taxonomy, which includes awareness, prevention, protection, response, and recovery.

[62] These include improving sensor performance; improving advance risk modeling, simulation, and analysis for decision support; improving cyber security; improving prevention and protection; improving situational awareness for critical infrastructures; developing next-generation designs and architectures for CI/KR protection-related devices and systems; and developing human-technology interfaces that allow better comprehension and decisions concerning CI/KR protection-related factors.

CI/KR Protection R&D at the State, County, Local, and Tribal Levels. At the State and local level, the R&D activity related to CI/KR protection, though largely unknown, is likely to be small. Most State and local agencies have limited R&D programs.[63] In the past, few have regarded themselves as possessing CI/KR that are subject to attack, apart from limited facility protection incidents common in every sector of the economy. Tribal entities are believed unlikely to conduct CI/KR protection-related R&D. A few large cities, such as New York and Los Angeles, may have limited CI/KR protection-related research programs. During 2007, HHS will, in concert with its security partners, investigate these measures further.

CI/KR Protection R&D in the Private Sector. The Healthcare and Public Health Sector supports extensive R&D focused on medical products and services. It is believed to devote relatively few resources to CI/KR areas. Large healthcare corporations with major manufacturing and storage capability do invest in CI/KR protection and, to some extent, in CI/KR protection R&D. Little information is currently available on the content of such programs. Given its proprietary or otherwise sensitive nature, information on these programs will need to be gathered in close coordination with the SCC in 2007.

Investigations are planned in consultation with the SCC during the upcoming year. Approximately 92 percent of the overall Healthcare and Public Health Sector is managed privately. This means that private sector CI/KR protection R&D could be an important component in the overall national picture.

7.1.5 Sector R&D Goals

In this context, major R&D goals of interest to the Healthcare and Public Health Sector will be developed by HHS in consultation with its Federal partners, the GCC, the SCC, and other security partners. At present, these goals include, but are not limited to, the following:

Developing Improved Ways to Protect the Healthcare and Public Health Workforce. This goal calls for the development of improved tools, equipment, and procedures to protect healthcare and emergency response personnel from the threats and hazards they are likely to encounter in meeting their responsibilities during terrorist-related emergencies and other hazardous conditions.

Improving Vaccine Development. This goal requires the development of improved methods for ensuring a reliable, continuing supply of vaccines to deal with bio-threats of all kinds, including natural epidemics and manmade health threats. Methods are sought that are effective despite the lack of market incentives prompting the private sector to produce them.[64]

Developing Improved Biosensors. This goal encompasses the development of improved sensors for use in urban areas to detect the presence of hazardous substances that might be used by terrorists (e.g., chemical, biological, and radiological weapons) against humans, animals, foods, or combinations thereof. It also encompasses the development of improved sensors for rural areas to detect the presence of biohazards that might be used by terrorists against agricultural targets to attack the food supply.

Developing Improved Bio-Countermeasures. This goal includes the development of improved countermeasures for each of the biohazards mentioned above when these hazards could plausibly be incurred in urban or rural attacks.

Developing Improved Cyber Attack Detection and Countermeasures. Among the possible goals under this heading are assessments of the key threats to emerging electronic commerce, including electronic health records, in the Healthcare and Public Health Sector. This goal also includes the development of countermeasures that might be taken by those within the sector to ensure the safety and security of key networks and processes.

Improving the Development of Medical Materiel for Use in Selected Emergencies. This goal encompasses the identification of specialized medical materiel that may be needed in the event of terrorist attacks or other national emergencies that is not produced

[63] There are exceptions, of course, including California, New York, and perhaps others.

[64] Though not necessarily an R&D subject, reviewers have suggested that additional legal protection might be required for potential vaccine manufacturers.

by the private sector as a result of such market factors as low volume or low profitability. It also includes developing ways to promote the R&D needed in the private sector to develop and produce medical materiel appropriate to certain kinds of emergencies.

Improving CI/KR Protection Technology Transfer. This goal involves the investigation of methods for ensuring successful transfer of CI/KR protection-related R&D results into usable products for common use within the Healthcare and Public Health Sector to help protect CI/KR.

Strengthening Surge Capacity Modeling Tools. This goal involves the development of models and technology to address surge capacity of a region by linking real-time data on hospital beds, emergency department censuses, equipment, supplies, and personnel. Automated tools must be able to handle various scenarios involving different biohazards, illnesses, injuries, and ages of patients.

Strengthening Real-Time CI/KR Protection Data Gathering and Analysis Tools. This goal involves the development of tools for gathering real-time data on critical infrastructures involved in significant destructive events affecting the sector on a regional or national basis. Such tools would be useful in monitoring the situation in the affected areas with a view to identifying post-event damage to healthcare and public health capabilities. This, in turn, would help identify emergency needs that Federal agencies could meet.

Table 7-1 maps these goals against national CI/KR protection R&D themes. These goals cannot all be accomplished using HHS R&D resources alone. Consistent with the overall national concept, many of these goals can only be accomplished by drawing on the R&D efforts of other Federal agencies and private sector entities.

Table 7-1: HHS R&D Goals Mapped to National CI/KR Protection R&D Themes

HHS R&D Initiatives	Summary	Applicable National R&D Themes[70]
Protection of the Healthcare and Public Health Workforce	Focuses on improved tools, equipment, and procedures, including allocation of vaccines, to protect healthcare and emergency response personnel during terrorist-related emergencies and other hazardous conditions.	• Detection and sensor systems; • Protection and prevention; • Entry and access portals; • Insider threats; and • Human and social issues.
Improved Vaccine, Antiviral, and Antimicrobial Development	Development of improved methods for ensuring a reliable, continuing supply of vaccines to deal with bio-threats.	• Response, recovery, and reconstitution; • New and emerging threats and vulnerabilities; and • Human and social issues.
Biosensor and Countermeasure Development	Development of improved sensors for use in urban areas to detect the presence of hazardous substances.	• Detection and sensor systems; • Protection and prevention; • Entry and access portals; • Insider threats; • Analysis and decision support systems; • Response, recovery, and reconstitution; • New and emerging threats and vulnerabilities; and • Human and social issues.

[65] These themes are identified in the Executive Office of the President, Office of Science and Technology Policy, and DHS, Science and Technology Directorate, *The National Plan for Research and Development in Support of Critical Infrastructure Protection, Executive Summary*, p. v

HHS R&D Initiatives	Summary	Applicable National R&D Themes[70]
Cyber Threat Detection and Countermeasure Development	Assessments of key threats to emerging electronic commerce imposed by terrorists and other threatening parties.	• Detection and sensor systems; • Protection and prevention; • Insider threats; • Analysis and decision support systems; • Response, recovery, and reconstitution; • New and emerging threats and vulnerabilities; • Advanced infrastructure architectures and systems designs; and • Human and social issues
Medical Materiel Requirements	Identification and development of medical materiel needed during certain terrorist attacks, but not produced by the private sector.	• Response, recovery, reconstitution; • New and emerging threats and vulnerabilities; and • Human and social issues
Surveillance	Real-time incident reporting of infectious diseases and diseases of unknown origin.	• New and emerging threats and vulnerabilities; and • Detection and sensor systems
Technology Transfer	Investigation of methods for ensuring successful transfer of CI/KR protection-related R&D results into usable products for commercial production.	• Detection and sensor systems; • Entry and access portals; • Insider threats; • Analysis and decision support systems; • Response, recovery, and reconstitution; • New and emerging threats and vulnerabilities; and • Human and social issues.
Surge Capacity Modeling Tools	Development of models and technology to address surge capacity of a region by linking real-time data on hospital beds and emergency department censuses.	• Analysis and decision support systems; • Response, recovery, and reconstitution; and • Human and social issues
CI/KR Protection Data Gathering and Analysis Tools	Development of tools for gathering real-time data on infrastructures involved in destructive events affecting the system as whole.	• Analysis and decision support systems; and • Response, recovery, and reconstitution.

7.2 Healthcare and Public Health Sector CI/KR Protection R&D Technology Requirements

The Healthcare and Public Health Sector is not necessarily viewed as a target of terrorist attack; however, some sector elements could face such attacks. Moreover, no sector element is immune from other hazards, both natural and manmade. CI/KR protection R&D requirements must take both major sector functions into account. HHS, in coordination with its security partners, developed high-level requirements and, through the partnership model, will work to refine them further in 2007. Technology solutions should meet the following requirements:

- Affordable for a wide range of healthcare and public health facilities;

- Readily deployable by busy healthcare and public health facility staff at any level;
- Relatively simple maintenance requirements;
- Useful against a wide range of threats facing the sector;
- Durable under both routine and emergency conditions;
- Reliable under all conditions; and
- Readily interoperable with systems likely to be in place already.

7.3 Healthcare and Public Health Sector CI/KR Protection R&D Plan

Since several GCC members (e.g., HHS, DoD, and VA) play major healthcare and public health roles at the Federal level, these departments will collaborate in reviewing Federal R&D initiatives that relate to CI/KR protection issues. In this way, they can pool their expertise, identify gaps, verify overlaps where appropriate, and identify shared funding opportunities on topics of joint interest. Based on this assessment, they can determine which initiatives will have the greatest impact (e.g, which will have the potential to close major gaps).

In this effort, the GCC can draw on State, local, and private sector constituents for advice on R&D priorities based on the constituents' respective experiences. Such constituents could include ASTHO and NACCHO, and other public partners on the GCC, and the SCC and its subcouncils in the private sector. In addition, joint public/private conversations may occur under the Critical Infrastructure Partnership Advisory Council (CIPAC) umbrella.

GCC member agencies can also consult with DHS, which is establishing a vigorous R&D program of its own. In particular, the DHS Science and Technology Directorate is developing a national R&D program to support homeland security efforts, including CI/KR protection.

7.3.1 Assembling a Composite View of Federal CI/KR Protection R&D Annually

An initial step toward annually assembling a composite view of Federal CI/KR protection R&D is to research and develop a comprehensive picture of current R&D that is relevant to CI/KR protection issues facing the sector. Much R&D, which could benefit the sector, has already been conducted by other Federal agencies. The process of assembling a composite picture of potential R&D projects of interest has already begun. Drawing heavily on the resources of OSTP, HHS has assembled a description of unclassified R&D projects conducted by all relevant Federal agencies during FYs 2004 and 2005 (table 7-2). Many of these R&D efforts bear on sector CI/KR protection needs.

Fiscal Years 2004 and 2005 have been chosen for two reasons. First, the results or end product of projects conducted during this period may now be available. Second, these projects provide a reliable basis for identifying both gaps and overlaps that may currently exist. Table 7-2 provides an overview of the range of Federal R&D that should be reviewed in detail for relevance, gaps, and overlaps.

7.4 R&D Management Processes

Managing R&D is a complex process. Among other things, this process must review overall Federal R&D efforts on a continuing basis, assess the relevance to sector CI/KR protection needs of R&D efforts wherever they are conducted, monitor the progress made by these efforts, assess their impact on sector goals if implemented, identify gaps to be filled, recommend R&D programs to fill these gaps, and update the sector's CI/KR protection R&D plan as needed. Consistent with DHS guidance, the sector's R&D management process is discussed under the following headings:

7.4.1 Sector R&D Governance

The sector plans to establish a collaborative body that will work through the CIPAC process to coordinate the overall R&D process. This body, composed of R&D specialists with appropriate skills for reviewing, cataloging, and coordinating R&D efforts, will be made up of representatives from:

- A government group made up of R&D specialists drawn from, or nominated by, members of the GCC;
- A private sector group composed of R&D specialists drawn from, or nominated by, members of the SCC; and
- An academic group composed of university researchers from the appropriate fields.

This body will be known as the Public/Private Healthcare and Public Health Sector CI/KR Protection R&D Governance Organization.

Table 7-2: Summary of Unclassified R&D Projects During FYs 2004 and 2005 by Topic Area (in Alphabetical Order)[66]

Overall R&D Topics[67]	Approximate Number of Projects[68]	Major Federal R&D Funding Agencies[69]
Agro-Terrorism: Detection of, Protection Against	57	U.S. Department of Agriculture (USDA), U.S. Department of Energy (DOE), DHS, HHS, U.S. Department of Environmental Protection (EPA), National Science Foundation (NSF), National Aeronautics and Space Administration (NASA), U.S. Postal Service (USPS)
Anthrax: Detection of, Protection Against	249	USDA, DoD, DOE, DHS, HHS, U.S. Department of Transportation (DOT), EPA, NSF, USPS
Bio-Weapons: Detection of, Protection Against	1,305	USDA, DoD, DOE, DHS, DOJ, HHS, EPA, NSF, NASA, USPS
Chemical Weapons: Threats of, Protection Against	778	USDA, U.S. Department of Commerce (DOC), DoD, DOE, DHS, HHS, DOT, EPA, NSF, NASA, USPS
Counterterrorism: Various Topics	20	USDA, DOC, DoD, DOE, DHS, DOJ, HHS, DOT, EPA, NSF, Nuclear Regulatory Commission (NRC), USPS
Cyber Security: Multiple Aspects of	3,889	DOC, DoD, DOE, DOT, NSF, NSA, DARPA
Emergency Medicine: Improving Technologies for Remote Conduct of	34	HHS, NASA
Explosives: Effects of, Defenses Against	447	DOC, DoD, DOE, DHS, HHS, NSF, USPS
Food: Threats Against, Protection of	678	USDA, DoD, DHS, HHS, NSF,
Healthcare Planning: Surge Capacity, Information Systems Protection, Worker Protection	555	HHS, NSF, DoD

66 From searches of multiple Federal R&D databases containing unclassified R&D projects using search criteria intended to identify R&D topics of relevance to the Healthcare and Public Health Sector objectives defined in this section of the SSP.

67 These broad categories were developed in consultation with the OSTP.

68 The term "approximate" refers to the fact that some R&D projects deal with multiple subjects, including, but not limited to, the topic indicated by the row heading.

69 Search criteria have been applied against the R&D programs sponsored by the Departments of Agriculture, Commerce, Defense, Energy, Homeland Security, Justice, Health and Human Services, Transportation, and Treasury. Also searched were the Environmental Protection Agency, the National Science Foundation, the Nuclear Regulatory Commission, the National Aeronautics and Space Administration, and the U.S. Postal Service. These search criteria have been based on the sector R&D goals described in Section 7.1.5.

Overall R&D Topics[67]	Approximate Number of Projects[68]	Major Federal R&D Funding Agencies[69]
Hostage Situations: Applicable Technologies for Responding to	11	DOJ
Homeland Security Hazard Detection: Tools for, Methods of	305	DoD, DHS, HHS, EPA, NSF, NASA
Impact of Terrorist Attacks on Individual Trauma Centers: Tools for, Methods for Assessing	260	DoD, DHS, HHS, EPA, NSF
Insider Threats: Types of, Gaps Likely, Mitigation of	195	NSF
Nuclear Attacks: Protection in the Event of, Response to	306	DoD, DOE, DHS, HHS, EPA, NSF, NRC
Pandemics: Detection of, Defense Against	25	USDA, DoD, DHS, HHS, EPA, NSF, USPS
Pathogens/Toxins: Investigation of, Significance in Hostile Environments	21	HHS, DoD
Radiological Attacks: Effects of, Defense Against	43	DoD, DOE, DHS, HHS, EPA, NSF, NRC, NASA
Terrorism: Threats Posed by, Protection Against	255	DOC, DoD, DOE, DHS, DOJ, HHS, DOT, EPA, NSF, NRC, NASA, USPS
Vaccines: Development of, Improvements in	310	NSF, DoD, HHS
Water: Attacks Against, Despoilment of	24	USDA, DoD, DOE, DHS, HHS, EPA, NSF, NRC, NASA, USPS
Total Projects to Review for Applicability	9,767	

7.4.2 Initial Tasking

The initial task of the CI/KR protection R&D Governance Organization will be to coordinate the cataloging of CI/KR protection-related R&D conducted by governmental and nongovernmental organizations, including universities and non-profit entities of various kinds, and to establish a mechanism for institutionalizing the governance process. Thereafter, the CI/KR Protection R&D Governance Organization will assume responsibility for the following continuing tasks:

- Solicit input from the GCC and SCC at appropriate junctures concerning CI/KR protection R&D efforts (existing, planned, or needed) that could be candidates for inclusion in the Federal CI/KR Protection R&D Plan or for private sector research;
- Develop a comprehensive view across the sector of relevant R&D efforts focused on CI/KR protection-related topics;
- Identify known or presumed CI/KR protection-related problems facing the sector that could be resolved or ameliorated through appropriate R&D programs not yet established;

- Recommend programs to the OSTP annually that will fill identified gaps; and
- Conduct all other investigations that may be needed to achieve overall HSPD-7 objectives for achieving a comprehensive National R&D Plan for CI/KR protection that, among other things, reflects sector needs and priorities.

7.4.3 Coordination with the CI/KR Protection R&D Community and with Other Sectors

The CI/KR Protection R&D Governance Organization will be responsible for coordination with all Federal, State, local, and tribal R&D efforts. It will also be responsible for coordinating with private sector R&D entities as applicable.

7.4.4 Progress and Impact of the Plan

On a continuing basis, the CI/KR Protection R&D Governance Organization will review progress, document the results, and evaluate the progress being made under the plan.

7.4.5 Technology Scanning

On a continuing basis, the CI/KR Protection R&D Governance Organization will be responsible for reviewing the evolution of applicable technologies and for assessing their likely applicability to the sector's CI/KR protection needs and requirements.

7.4.6 Technology Transition

On a continuing basis, the CI/KR Protection R&D Governance Organization will be responsible for identifying ways to incorporate new technologies emerging from the R&D process, and for recommending ways to promote the adoption of these emerging technologies throughout the sector, as appropriate.[70]

7.5 The Path Forward

In order to address the issues outlined in this section, the sector (GCC, SCC, and all relevant CI/KR protection partners) will need to undertake many tasks as the program matures. The list below addresses some of these. For the specific tasks to be undertaken in the coming year, refer to the table in section 6.2, Implementation Actions.

- Establish the CI/KR Protection R&D Governance Organization and assign it the tasks identified in this section of the SSP;
- Develop appropriate plans for carrying out these tasks in consultation with DHS, DoD, VA, OSTP, the sector GCC and SCC, and other relevant agencies, as appropriate; and
- Develop mechanisms for assembling the R&D data summarized in this section of the SSP on a continuing basis for use in the National CI/KR Protection R&D Plan.

[70] Legal issues may arise at various steps in the R&D process. These may include, but are not necessarily limited to, legal protection for developers of new CI/KR protection-related processes if unforeseen hazards to health and safety are encountered, or if new risks of other kinds are introduced. This topic lies outside the scope of this SSP, but are worthy of consideration as R&D plans and evaluations are encountered.

8. Managing and Coordinating SSA Responsibilities

This section describes the management processes that HHS is establishing to meet its responsibilities under HSPD-7 and related guidance. This section also describes information-sharing mechanisms that are used by the sector, as well as the processes, programs, and tools that each sector has in place to ensure protection of CI/KR information collected by HHS or its sector security partners. As required by DHS guidance, major topics in this section include the following:

- Program management approach;
- Processes and responsibilities;
- Implementing the sector partnership model; and
- Information sharing and protection.

8.1 Program Management Approach

HHS has placed overall authority for HSPD-7 in ASPR. ASPR has established a Program Office to manage its HSPD-7 responsibilities. This Program Office will continue to be supported by a contractor.

The overall philosophy of HHS is that it will coordinate CI/KR protection-related activities with its strategic partners. These include, but are not necessarily limited to, its sister Cabinet-level agencies with relevant responsibilities; all State and Territorial bodies with major healthcare and public health responsibilities; professional associations interested in CI/KR protection issues; and the private sector at all levels.

Since inception of HSPD-7, HHS has worked to establish, educate, and assemble a broad range of skills to manage NIPP-related responsibilities. As the sector's SSA, HHS believes that while short-terms goals must be met, long-term requirements are best achieved by employing a consistent, reliable group of staff long term. HHS staffing skills and expertise include project management, regulatory compliance, physical and cyber security, database design and development, knowledge management, healthcare (public and private sector), government, military, intelligence analysis, biosurveillance, network architecting, risk management/risk analysis, and clinical services.

8.2 Processes and Responsibilities

Key processes and responsibilities to be undertaken in service of overall HSPD-7 responsibilities are summarized below.

8.2.1 SSP Maintenance and Update

The SSP must be updated on a continuing basis in response to several factors. These include evolutions in DHS guidance, changes in organizational responsibilities among strategic partners, improvements in CI/KR protection-related knowledge, progress made in developing and implementing protective programs, and a host of other factors. For these reasons, the maintenance and update process is likely to involve many of the factors identified in DHS guidance. Among the most important factors necessitating updates to the SSP are the following:

- When there is a critical change in the definition of assets, system, networks, or the functions they provide to reflect the implications of those changes;
- Annually to reflect significant changes during the period since the last update;
- As part of completing the annual reporting requirements; and
- Whenever there is a major new initiative.

In general, the HHS objective is to keep the SSP current with the state-of-the-art in CI/KR protection for the sector. Within HHS, ASPR has version control over the SSP and is wholly responsible for maintaining it once the document is finalized for yearly submission. Only members of ASPR are permitted to make changes outside of the standard revision period. These changes can be made only with the approval of the Director of DHS' HSPD-7 Program.

The process for updating the SSP annually requires that SCC and GCC members submit their edits to the program team for review, reconciliation, and inclusion into the base document. This process ensures that a single, cohesive voice is maintained throughout each section and that all components of the document are addressed.

8.2.2 Annual Reporting

HHS has established a process for updating the Sector Annual Report based on its experience during 2006. The ASPR Program Office is authorized to maintain all necessary contacts with major strategic partners for annual report purposes.

The process for collecting information takes into consideration not only those resources that have responsibility for various aspects of infrastructure protection, but also academia and accreditation organizations that may influence or provide services for assessing and documenting protective activities. Hence, collection gathering typically includes research into current healthcare and public health activities (e.g., biosurveillance, the National Health Information Infrastructure, R&D, pharmaceutical issues); a review of protective programs under the jurisdiction of the SSA (e.g., HIPAA, various CI/KR within HHS); and a call for input from GCC, SCC, and other strategic partners, including DHS or programs sponsored by others.

8.2.3 Resources and Budgets

The HHS plan for managing resources and budgets acknowledges that the vast majority of sector assets lie outside HHS control. For this reason, HHS plans to deal with resource and budget issues in the following manner.

Designating Responsibilities. ASPR does not have line authority over the major operating divisions within HHS that contain or influence CI or KR. Therefore, ASPR intends to work with budget authorities in each of these operating divisions to suggest ways to formulate their budget requests to incorporate CI/KR protection resources as needed.

Developing Sector-Specific Investment Priorities and Requirements. Having developed a set of agreed-upon sector goals for CI/KR protection, prioritized CI and KR, and developed experience with protective programs, HHS will work with the sector GCC and SCC to establish investment priorities. These priorities will be published in appropriate forums as a means of gaining support among sector entities that HHS does not control, but which they can influence.

Identifying Resources for CI/KR Protection. Based on investment priorities and requirements, ASPR will work with HHS budget analysts to obtain resources in the annual budgeting process. ASPR will collaborate with appropriate HHS offices to secure funding for CI/KR protection activities and to allocate this funding to CI/KR protection activities, as appropriate.

Working to Obtain and Coordinate Resources Outside HHS. Based on the above results and other factors, HHS will collaborate fully with its partner agencies to secure the resources needed to achieve overall CI/KR protection-related requirements.

8.2.4 Training and Education

There is a need for appropriate training on CI/KR protection issues and problems across the entire Healthcare and Public Health Sector. Risk management, physical security, cost-benefit analysis, and cyber security are topics requiring greater emphasis under HSPD-7 in much of the sector as many sector entities are unfamiliar with the terminology and/or concentrate more closely on response. As sector efforts become better coordinated, training in topics such as the NIPP requirements, threat scenarios and assessment methods, and information-sharing mechanisms may be identified.

Training and Education External to HHS. Many CI/KR are owned and operated outside HHS. Therefore, HHS must encourage rather than mandate appropriate training and education. Several cost-effective strategies are being considered, including:

- Extensive use of professional journals to create awareness among sector professionals of CI/KR protection issues, problems, and threats;
- Extensive use of professional conventions and meetings to present papers with much the same overall purposes; and
- Selective sponsorship of workshops oriented toward CI/KR protection issues, problems, and best practices.

Training and Education within HHS. HHS has been working with its principal contractor as well as internal staff to ensure the appropriate depth and breadth of knowledge is developed within the HHS CI/KR protection program. Most of the immediate ASPR team already has a background in the key areas of homeland defense that achieve protection objectives. In addition, HHS has its own security training program that relevant personnel are required to take annually.

Beyond the standard training programs and expertise that exists within HHS, team members are encouraged to take follow-on classes through the FEMA Emergency Management Institute (EMI). The training has been useful in educating staff across multiple disciplines and ensuring continuity of support during peak vacation periods. EMI training has two major characteristics:

- Provides individuals a strategic view of the activities necessary to promote the response activities that are required for CI/KR protection; and
- Addresses many important topics, ranging from change management to incident command management.

These training programs are made available to private sector staff as well as Federal employees. The contributions and effectiveness of individuals to the HSPD-7 program have increased as a result of the training.

8.3 Implementing the Sector Partnership Model

As summarized in the 2006 Sector Annual Report, the Healthcare and Public Health Sector is highly decentralized. Implementation of the sector partnership model requires the development of sector-unique implementation strategies in many cases.

8.3.1 NIPP Coordination Councils

As the SSA for the sector, HHS is fully supportive of the coordination councils envisioned in the NIPP.

National Councils: HHS is a participant in the GCC and the Government Cross-Sector Council established by the NIPP. As these organizations mature, HHS plans to represent the interests and concerns of the Healthcare and Public Health Sector in the deliberations of these new bodies.

Government Coordinating Council: HHS initiated a GCC as required by DHS guidance in early 2004. It has met quarterly with the SCC (discussed below) since December 2005, and it has authored a charter that establishes its overall membership and activities. The GCC has accepted and carried out several tasks over the entire 2-year period (e.g., reviewed drafts of the SSP in each of the first 2 years and made invaluable contributions to its development).

In June 2006, HHS undertook an effort to obtain greater involvement from all agencies and government stakeholders with an interest in critical infrastructure protection in the sector. Through this wider partnership, the GCC brings to bear the combined expertise of Federal, State, local, and tribal governments with respect to CI/KR protection issues and problems. GCC representatives are responsible for reaching back into their organizations for subject matter expertise, as necessary, to address issues as they arise. A list of GCC member organizations can be found in Appendix 6.

Sector Coordinating Council: The sector's SCC was initially established in fall 2003 and met periodically. On June 7, 2006, the SCC agreed to revisit its organization and operation at the request of HHS and DHS. Subsequent to that meeting, the SCC has revisited membership and structural issues and is moving in a direction that recognizes its desire to work closely with government, yet allows it to operate on its own as an independent representative of the sector's owners and operators.

The SCC has organized itself functionally around nine sub-councils. These include Medical Materiel Coordination; Pharmaceuticals and Biotechnology; Occupational Health; Healthcare Personnel; Medical Treatment; Laboratories and Blood; Mass Fatality Management; Information Technology; and Insurers, Payers, and HMOs. A list of SCC member organizations can be found in appendix 6.

8.3.2 State, Local, and Tribal Government Coordinating Bodies

HHS has worked through two major State and local healthcare and public health professional associations to establish appropriate links with the State and Territorial public health bodies. NACCHO and ASTHO have long-standing linkages with both HHS and their respective memberships. The two-way communication that can be fostered through these bodies has worked well. Both organizations are represented on the GCC.

Organizationally, the Indian Health Service resides within HHS and assists in communication with tribal health councils. CI/KR protection-related dialogue with two national tribal representative organizations is in place and the National Indian Health Board has participated in GCC meetings. The dialogue will continue during the upcoming year to strengthen tribal engagement in CI/KR protection issues.

8.3.3 International Coordinating Bodies

Although the sector is largely confined to the United States, it has many connections with international bodies. At the Federal Governmental level, this includes bilateral ties with Canada and Mexico concerned with, among other things, health-related border issues. The Federal Government also maintains many ties with international organizations with health-related responsibilities (i.e., the World Health Organization, Pan American Health Organization, World Organization for Animal Health, Food and Agriculture Organization, Asia-Pacific Economic Cooperation Forum, etc.). There are comparatively few CI/KR protection-related ties of the kind identified in the guidance (e.g., there are few healthcare and public health critical infrastructures "on or near the borders," and there are few "international interdependencies and vulnerable nodes").

In the private sector, many suppliers of medically related products and equipment are multi-national corporations. Many of these have production and distribution facilities in Puerto Rico and elsewhere outside the continental United States. The CI/KR protection consequences of such multi-national suppliers, if any, require further exploration.

8.4 Information Sharing and Protection

As the 2006 NIPP makes clear, effective sharing of CI/KR protection-related information is a cornerstone of effective CI/KR protection planning and execution. Many information-sharing mechanisms are already at work within the sector, creating a foundation for building on in the upcoming year as discussed below.

8.4.1 Information Sharing in the Sector

HHS and its many strategic partners already share various forms of information across the sector, particularly in connection with healthcare and public health topics. The information-sharing mechanisms already in place are not specifically focused on CI/KR protection topics, but can be leveraged to convey such information or augment the critical infrastructure information-sharing process. However, there is still the need to better coordinate these various mechanisms to meet the intent of the NIPP.

Sector security partners at all levels of government and in the private sector play a role in providing and consuming information related to CI/KR protection. HHS recognizes that owners, operators, and other stakeholders in the Healthcare and Public Health Sector have the greatest understanding of their own physical and cyber assets, systems, and networks. Hence, collaboration between owners and operators and government entities is vital in defining the most efficient and appropriate ways to share infrastructure protection information. In addition to acting as an information-sharing forum, the GCC and the SCC must:

- Identify information-sharing processes that enhance cross-sector collaboration and communications and protective mechanisms to safeguard voluntary private-sector information;
- Improve threat pre-emption and response capabilities that can be strengthened by government and private sector collaboration; and
- Increase the probability of neutralizing crises before they occur by increasing communication among sector partners on CI/KR protection-related issues and threats.

Section 4 of the NIPP portrays an overall nodal concept for information sharing, and the Healthcare and Public Health Sector fits within this model. Looking from the bottom up, it is important that Federal, State, and local governments receive good information from owners and operators. This information includes reports of suspicious activity; operational and vulnerability information; situational awareness information (e.g., relating to biosurveillance, hospital capacity) that can assist in the allocation of resources; and subject matter expertise in areas related to specific infrastructure protection issues.

There are many mechanisms that already collect these types of information from owners and operators. Situational awareness systems range from State and local hospital status systems (e.g., New York's Hospital Emergency Response Data System, EMSystem, etc.) to National-level biosurveillance initiatives (e.g., BioSense). More examples can be found in table 8.1. Suspicious activity reports are made through calls to law enforcement and by contacting appropriate emergency operating centers. In addition, owners and operators share information on vulnerabilities and the status of facilities through regulatory channels, as part of collaborative planning efforts and as part of assessments and data calls requested by government entities.

Taking a top-down view, there is also the need for government entities to communicate useful, actionable information to its security partners. There are many sector mechanisms that are in place to do this as well. For example, the Health Alert Network (HAN) is a system that allows for targeted alerts to be sent out to various user communities; the Epidemic Information Exchange (Epi-X) allows the quick and secure sharing of preliminary health surveillance information with public health professionals; for cyber matters, US-CERT ensures that government-developed threat information is sent expeditiously to owners and operators of publicly and privately occupied facilities. Again, a more comprehensive list of examples can be found in table 8-1. In addition, HITRAC promulgates sector-targeted threat information that can be shared with owners and operators.

Given the activity within the sector to collect and promulgate information, there are opportunities to better coordinate the overall information-sharing picture. At a high level, the nexus for information sharing within DHS is the National Operations

Center (NOC). Within NOC, the National Infrastructure Coordination Center (NICC) coordinates the collection and dissemination of suspicious activity reports and threat information and acts to coordinate CI/KR protection efforts during emergencies. Within HHS, the Secretary's Operations Center (SOC) serves to assist the Secretary in maintaining situational awareness of healthcare and public health matters and coordinates sector efforts under Emergency Support Function-8 of the National Response Plan. The NOC and the SOC are linked to other Federal, State, and local information-collection and -sharing systems and act to analyze and disseminate information useful to overall protective efforts. In addition, both organizations have regional representatives and place personnel at the Joint Field Office during events to work with State and local governments and owners and operators. Efforts to formalize the collaboration between the NOC and the SOC are underway.

In addition to the work being done at and between operations centers, there is still the need to facilitate the partnership model and ensure that there is a way for owners and operators and government security partners to collaborate and share information. DHS developed the HSIN-CS to provide a portal for this purpose and the sector has piloted the system. In 2007, the sector plans to move from the pilot to implementation of HSIN for use in gathering information, and collaborating and disseminating useful information back to sector security partners.

Despite the useful activities being pursued within the sector, there is still work to be done to coordinate the disparate information flows into a more cohesive whole. Working through the partnership model, the sector will continue to address these issues in the coming year.

8.4.2 Information Protection

Many in the private healthcare sector see disincentives in providing information. These disincentives include: concerns about the protection of proprietary data; fears about increasing regulation; apprehensions about loss of competitive advantage resulting from the inappropriate or inadvertent disclosure of proprietary data; skepticism about the uses to which government agencies may put the data, both now and in the future; and, concerns about the resources that might be necessary to fulfill the desires of government partners. As the NIPP points out, the private sector's role in information collection is largely voluntary due to antitrust considerations, privacy concerns, competitive advantage imperatives, and other factors. Nonetheless, private sector counsel is crucial to success. As outlined earlier in the document, there are programs in place, such as PCII, to help protect private sector information, and HHS and DHS are working to implement such programs for the sector.

In addition, there is a need, from the government side, to ensure that information that could be potentially sensitive or classified be protected from improper disclosure or distribution. Owners and operators have requested more timely and actionable information, and HHS and DHS will work together with other governmental partners to develop procedures (e.g., the development of better unclassified threat products) to ensure that appropriate information can be shared with owners and operators that is respectful of information security.

Table 8-1: Selected Information-Sharing Systems and Networks (in Alphabetical Order)[71]

Name	Operator	Overall Purpose
BioSense	CDC	Syndromic surveillance system involving data from Federal healthcare facilities and more than 10,000 over-the-counter retailers that may indicate the emergence of an infectious disease outbreak.
BioWatch	CDC	Samples of air in various cities to detect biohazards of various kinds.

[71] Adapted from Report to the Chairman, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate, Emerging Infectious Diseases: Review of State and Federal Disease Surveillance Efforts, GAO-04-877, September 2004, Appendix III.

Name	Operator	Overall Purpose
Electronic Laboratory Exchange Network	FDA, USDA, and U.S. Army Pacific Region Food Analysis Laboratory	Web-based system for real-time sharing of food safety laboratory data among Federal, State, and local agencies (113 laboratories in 50 States) as a means to deal with possible infectious disease outbreaks.
Electronic Surveillance System for the Early Notification of Community-based Epidemics	DoD	Syndromic surveillance system involving data from multiple sources that can be used in the early detection of infectious disease outbreaks and provide epidemiological tools for improved investigation.
EMSystem	Sector Participants	Hospital-to-hospital communications system used in more than 30 percent of all acute care hospitals to share information of interest.
Epidemic Information Exchange (Epi-X)	CDC	Web-based communications system operating in all 50 States to share disease outbreak information with State and local public health officials.
Foodborne Disease Active Surveillance Network (FoodNet)	CDC, FDA, and USDA	Operates in nine States, providing a network for responding to new and emerging foodborne diseases of national importance.
Global Outbreak Alert and Response Network	WHO	Electronically links WHO member countries and their respective disease experts, agencies, and laboratories to keep them informed of disease outbreaks, either rumored or confirmed.
Global Public Health Intelligence Network	WHO	An Internet-based application that searches in French and English more than 950 news feeds and discussion groups for information on possible outbreaks of infectious diseases.
Health Alert Network (HAN)	CDC	Network for issuing health alerts to an estimated 1 million public health officials, including physicians, nurses, laboratory staff, and others.
Infectious Diseases Society of America Emerging Infections Network	Infectious Disease Society	Means for surveying members regularly on topical issues in clinical infectious diseases.
Laboratory Response Network	CDC	Network linking public health and clinical laboratories to test specimens and develop diagnostic tests for identifying infectious diseases and biological or chemical agents.
National Animal Health Laboratory Network	USDA, U.S. Animal Health Association, American Association of Veterinary Laboratory Diagnosticians, participating States	Network linking laboratories supporting State veterinarians and others in participating States with regard to confirming animal diseases (including those with human significance) of major significance in livestock, poultry, and aquaculture species in the United States.
National Animal Health Reporting System	USDA, U.S. Animal Health Association, American Association of Veterinary Laboratory Diagnosticians, participating States.	Collects data from State veterinarians in participating States on the confirmed clinical diseases (including those with human significance) of major international significance in livestock, poultry, and aquaculture species in the United States.

Name	Operator	Overall Purpose
National Electronic Disease Surveillance System (NEDSS)	CDC	Intended to replace or enhance the interoperability of CDC's numerous existing surveillance systems. Includes ready-to-use software for the system known as the NEDSS Base System (National Biosurveillance Integration System).
National Electronic Telecommunications System for Surveillance (NETSS)	CDC	Computerized public health surveillance system providing CDC with weekly data regarding cases of nationally notifiable diseases. NETSS will be phased out as NEDSS is phased in.
National Healthcare Safety Network	CDC	System to monitor infections and other adverse health events.
National Retail Data Monitor	University of Pittsburgh and others	A syndromic surveillance system that collects sales data from 19,000 stores, including pharmacies, to monitor over-the-counter medication for signs of a developing infectious disease outbreak.
National Veterinary Services Laboratories (NVSL)	USDA	The only Federal veterinary reference laboratories to provide diagnostics for domestic and foreign animal diseases. Provides diagnostic support for disease control and eradication programs.
National Disaster Medical System (NDMS)	HHS	Supports Federal agencies in the management and coordination of the Federal medical response to major emergencies and federally declared disasters.
PulseNet	FDA, CDC	A national network of public health laboratories that perform DNA "fingerprinting" on bacteria that may be foodborne as a means of supporting early warnings concerning foodborne diseases.
Real-Time Outbreak and Disease Surveillance	University of Pittsburgh	Automatically gathers data from hospital clinical encounters to identify patients' chief medical complaints, classify them according to syndrome, and aggregate them to help identify possible emerging outbreaks.
Systematic Tracking of Elevated Lead Levels and Remediation	CDC	Electronic system used by State and local health departments to report lead poisoning cases to the CDC.
Vaccine Ordering and Distribution System	CDC	Part of the Vaccine Management Business Improvement Project as the mechanism to track pandemic influenza vaccines.

8.5 The Path Forward

In order to address the issues outlined in this section, the sector (GCC, SCC, and all relevant CI/KR protection partners) will need to undertake many tasks as the program matures. The list below addresses some of these. For the specific tasks to be undertaken in the coming year, refer to the table in section 6.2, Implementation Actions.

8.5.1 Strengthening Program Management

- Continue to strengthen program management capabilities with respect to HSPD-7 responsibilities; and
- Create and/or formalize appropriate structures within the Office of Assistant Secretary for Preparedness and Response to carry out these responsibilities.

8.5.2 Implementing the Sector Partnership Model

- Strengthen CI/KR protection-related information-sharing capabilities among Federal, State, local, and tribal government, and between these bodies and the private sector;
- Update procedures for handling sensitive information, including classified and PCII information, across organizational boundaries, as needed; and
- Revise existing structures and procedures for dealing with governmental and private sector partners, as needed, in light of experience to date, and in consultation with these strategic partners.

8.5.3 Information Sharing

- Establish more cohesive, sector-specific information-sharing mechanisms.

Appendix 1: List of Acronyms and Abbreviations

AFMIC	Armed Forces Medical Intelligence Center
ASIS	American Society for Information Science
ASPR	The Office of the Assistant Secretary for Preparedness and Response
ASTHO	Association of State and Territorial Health Officials
BZPP	Buffer Zone Protection Program
C&A	Certification and Accreditation
CBRN	Chemical, Biological, Radiological, and Nuclear
CDC	Centers for Disease Control and Prevention
CFR	Code of Federal Regulations
CI	Critical Infrastructure
CI/KR	Critical Infrastructure and Key Resources
CII	Critical Infrastructure Information
CIPAC	Critical Infrastructure Partnership Advisory Council
COBIT	Control Objectives for Information and Related Technology
COOP	Continuity-of-Operations Plan
CSEA	Cyber Security Enhancement Act
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DOC	Department of Commerce
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOL	Department of Labor
DOT	Department of Transportation
EMI	Emergency Management Institute
EPA	Environmental Protection Agency
Epi-X	Epidemic Information Exchange
ESF	Emergency Support Function
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act
FoodNet	Foodborne Diseases Active Surveillance Network
FPC	Federal Preparedness Circular
FY	Fiscal Year
GCC	Government Coordinating Council
GNP	Gross National Product
HAN	Health Alert Network
HEAT	Hospital Emergency Analysis Tool
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center

HMO	Health Maintenance Organization
HRSA	Health Resources and Services Administration
HSC	Homeland Security Council
HSIN	Homeland Security Information Network
HSIN-CS	Homeland Security Information Network-Critical Sector
HSPD	Homeland Security Presidential Directive
ICU	Intensive Care Unit
IFIP	Interagency Forum for Infrastructure Protection
ISO	International Organization for Standardization
IT	Information Technology
JCAHO	Joint Commission on Accreditation of Healthcare Organizations
KR	Key Resource
LAN	Local Area Network
MSA	Metropolitan Statistical Area
NACCHO	National Association of County and City Health Officials
NADB	National Asset Database
NASA	National Aeronautics and Space Administration
NCIP	National Critical Infrastructure Protection
NCQA	National Committee for Quality Assurance
NDMS	National Disaster Medical System
NEDSS	National Electronic Disease Surveillance System
NETSS	National Electronic Telecommunications System for Surveillance
NICC	National Infrastructure Coordination Center
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NOC	National Operations Center
NRC	Nuclear Regulatory Commission
NRP	National Response Plan
NSA	National Security Agency
NSF	National Science Foundation
NVSL	National Veterinary Services Laboratories
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OMB	Office of Management and Budget
OPEO	Office of Preparedness and Emergency Operations
OSHA	Occupational Safety and Health Administration
OSTP	Office of Science and Technology Policy
PCII	Protected Critical Infrastructure Information
PCIS	Partnership for Critical Infrastructure Security
PDD	Presidential Decision Directive
PHAST	Primary Health Assets Staging Tool
PHS	Public Health Service
PHTEA	Public Health Threats and Emergencies Act
PSI	Pharmaceutical Security Institute
RAMCAP	Risk Analysis and Management for Critical Asset Protection
SCC	Sector Coordinating Council
SHIRA	Strategic Homeland Infrastructure Risk Assessment
SOC	Secretary's Operations Center
SOCC	Secure One Communication Center
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USDA	Department of Agriculture
USGS	U.S. Geological Survey
USPS	United States Postal Service
VA	Department of Veterans Affairs
VHA	Veterans Health Administration
VLAN	Virtual Local Area Network
WHO	World Health Organization
WMD	Weapon of Mass Destruction

Appendix 2: Glossary

All-Hazards. An approach for prevention, protection, preparedness, response, and recovery that addresses a full range of threats and hazards, including domestic terrorist attacks, natural and manmade disasters, accidental disruptions, and other emergencies.

Asset. Contracts, facilities, property, electronic and non-electronic records and documents, balances of appropriations not obligated or expended, and other funds or resources (other than personnel).

Business Continuity. The ability of an organization to continue to function before, during, and after a disaster.

Consequence. The result of a terrorist attack or other hazard that reflects the level, duration, and nature of the loss resulting from the incident. For purposes of the National Infrastructure Protection Plan (NIPP), consequences are divided into four main categories of impact: public health and safety, economic, psychological, and governance.

Control Systems. Computer-based systems used within many infrastructures and industries to monitor and control sensitive processes and physical functions.

Cost/Benefit. Ratio of the cost of an option to the benefits it produces.

Cost Effectiveness. Ratio of the cost of an option to the measured progress it makes toward defined objectives.

Critical Infrastructure. Assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination thereof.

Cyber Security. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability.

Dependency. The one-directional reliance of an asset, system, network, or collection thereof within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

GCC. The Government Coordinating Council is the government counterpart to the Sector Coordinating Council (SCC) for each sector established to enable interagency coordination.

Hazard. Something that is potentially dangerous or harmful, often the root cause of an unwanted outcome.

Incident. An occurrence or event, natural or human-caused, that requires an emergency response to protect life or property.

Information Systems (44 United States Code (U.S.C.) 3502) (OMB Circular A-130, Appendix III). A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole.

Interdependency. The multi- or bi-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Key Resources. As defined in the Homeland Security Act, "key resources" are publicly or privately controlled resources essential to the minimal operations of the economy and government.

Mitigation. Activities designed to reduce or eliminate risks to persons or property or to lessen the actual or potential effects or consequences of an incident.

Normalize. In the context of the NIPP, the process of transforming risk-related data into comparable units.

Opportunity Cost. The cost of selecting an option in terms of the benefit foregone by not choosing the next best option.

Owner/Operators. Those entities responsible for day-to-day operation and investment in a particular asset or system.

Pandemic Flu (Influenza). A pandemic is a global disease outbreak. A Pandemic Flu occurs when a new influenza virus emerges for which people have little or no immunity, and for which there is no vaccine. The disease spreads easily from person-to-person, causes serious illness, and can sweep across the country and around the world in very short time.

Preparedness. The range of deliberate critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents.

Prevention. Actions taken to avoid an incident or to intervene to stop an incident from occurring.

Prioritization. The process of using risk assessment results to identify where risk-reduction or mitigation efforts are most needed.

Protection. Actions to mitigate the overall risk to critical infrastructure and key resources (CI/KR) assets, systems, networks, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation.

Recovery. The development, coordination, and execution of service- and site-restoration plans for impacted communities and the reconstitution of government operations and services through individual, private sector, nongovernmental, and public assistance programs that identify needs and define resources.

Resiliency. The ability of an asset, system, or network to maintain its functionality during, or to recover from, a terrorist attack or other incident.

Response. Activities that address the short-term, direct effects of an incident, including immediate actions to save lives, protect property, and meet basic human needs.

Risk. A measure of potential harm that encompasses threat, vulnerability, and consequence.

Risk Framework. A planning methodology that outlines the process for setting security goals; identifying assets, systems, networks, and functions; assessing risk; prioritizing and implementing protective programs; measuring performance; and taking corrective action.

SCC. The Sector Coordinating Council is the private sector counterpart to the public sector GCC. These councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. SCCs serve as the government's principal point of entry into each sector for developing and coordinating a wide range of CI/KR protection activities and issues.

Sector. A logical collection of assets, systems, workforces, or networks that perform a common function for the economy, government, or society.

Sector-Specific Agency. Federal departments and agencies identified in Homeland Security Presidential Directive 7 (HSPD-7) as responsible for CI/KR protection activities in specified CI/KR sectors.

Sector-Specific Plan. Augmenting plans that complement and extend the NIPP Base Plan and detail the application of the NIPP framework specific to each CI/KR sector.

Steady-State. The posture for routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents.

Threat. The intention and capability of an adversary to undertake actions that would be detrimental to CI/KR.

Value Proposition. A statement that outlines the National and homeland security interest in protecting the Nation's CI/KR and articulates benefits gained by all security partners through the risk management framework and public-private partnership described in the NIPP.

Vulnerability. A weakness in the design, implementation, or operation of an asset, system, or network that can be exploited by an adversary, or be disrupted by an attack or a natural hazard or technological failure.

WMD. Weapons of mass destruction include: (a) any explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than four ounces, missile having an explosive or incendiary charge of more than one-quarter ounce, or mine or similar device; (b) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors; (c) any weapon involving a disease organism; or (d) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

Appendix 3: Review of Authorities

Consistent with DHS guidance for 2006, this appendix identifies CI/KR protection-related Federal, State, and local authorities. The purpose is to summarize the major laws, rules, regulations, executive orders, and other guidance applicable to the protection of sector CI/KR.

3.1 Federal Authorities

This section summarizes the authorities of sector-specific Federal agencies playing some role in the healthcare and/or public health sector under defined circumstances. These authorities are grouped according to the following functions:

- Responding to bioterrorism;
- Responding to other WMDs;
- Ensuring cyber security;
- Promoting information sharing;
- Protecting information;
- Developing and promulgating plans;
- Protecting critical infrastructure;
- Conducting R&D;
- Providing Federal assistance to State and local authorities;
- Protecting freedom and privacy; and
- Protecting workforce personnel.

Table A3-1 summarizes key authorities by title. Given the complexity of these authorities, they are not summarized in detail. Instead, reviewers are invited to use the table as a checklist to be consulted when considering the legal framework for dealing with an issue identified in the Types of Authorities column.

Table A3-1: Summary of Major Federal Authorities by Agency and Key Functions: Healthcare and Public Health Sector

Types of Authorities	Laws, Regulations, Executive Orders, and Other Authorities
Authorities of Sector-Specific Agencies	
HHS	• Public Health Service Act of 1944 (42 United States Code (U.S.C.) 201-300hh-11), as amended; • Social Security Act of 1935 (42 U.S.C. 1320b-5), as amended; • Federal Food, Drug, and Cosmetic Act of 1938 (21 U.S.C. 301, et seq.), as amended; • Public Health Threats and Emergencies Act of 2000 (Title I of the Public Health Improvement Act (Public Law 106-505)); • Executive Order 13228 establishing the Homeland Security Council, including the Medical and Public Health Preparedness Policy Coordinating Committee; and • HSPD-7 18(b) designating HHS as the SSA for healthcare, public health, and food (other than meat, poultry, and egg products).
Department of Agriculture (USDA)	• HSPD-7 18(a) designating USDA as the SSA with respect to critical infrastructure protection for meat, poultry, and egg products, but not other foods.
Authorities Related to Critical Infrastructure Protection	
Responding to Bioterrorism	• Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458); • Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Public Law 107-188); • Title VIII, Section 817, of the USA Patriot Act of 2001 (Public Law 107-56); • Department of Veteran Affairs Emergency Preparedness Act of 2002 (Public Law 107-287); • Project BioShield Act of 2004 (Public Law 108-276); • Veterans Affairs Department and Department of Defense Health Resources Sharing and Emergency Operations Act of 2002 (Public Law 97-174); • Public Health Service Act of 1944 (42 U.S.C. 201-300hh-11), as amended; and • Food, Drug, and Cosmetic Act of 1938 (21 U.S.C. 301, et seq.), as amended.
Responding to Other WMDs	• Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458); • Defense Against Weapons of Mass Destruction Act of 1996 (50 U.S.C. 40); and • Deputy Secretary of Defense, Implementation of the National Response Plan and the National Incident Management System, OSD 21913-05, November 29, 2005.
Ensuring Cyber Security	• Critical Infrastructure Protection Act of 2001 (Title III, Section 1016, of the USA Patriot Act); • Computer Fraud and Abuse Act of 1984 (18 U.S.C. 1030); • Communications Lines, Stations, or Systems Act of 2002 (18 U.S.C. 1362); • Computer Fraud and Abuse Act of 1984 (18 U.S.C. 1030), as amended by the Computer Abuse Amendments Act of 1994; • Executive Order 13130 establishing the National Infrastructure Assurance Council; • Executive Order 13231 establishing the President's Critical Infrastructure Protection Board; and • Presidential Decision Directive 75 (PDD-75) establishing a counterintelligence role in identifying and protecting critical national assets.

Types of Authorities	Laws, Regulations, Executive Orders, and Other Authorities
Promoting Information Sharing	• Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458); • Homeland Security Information Sharing Act (Public Law 107-296), enacted as part of the Homeland Security Act of 2002; • Executive Order 13311 declaring the President's intent to promote information sharing; • Public Health Service Act of 1944 (42 U.S.C. 201-300hh-11), as amended; • Social Security Act of 1935 (42 U.S.C. 1320b-5), as amended; and • Federal Food, Drug, and Cosmetic Act of 1938 (21 U.S.C. 301, et seq.), as amended.
Protecting Information	• Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act); • Electronic Communications Privacy Act of 1986 (18 U.S.C. 2510); • Cyber Security Enhancement Act of 2002 (Title II, Section 225, of the Homeland Security Act of 2002); • Federal Information Security Management Act (Public Law 107-347), Title III of the E-Government Act of 2002; • Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191); • DHS Procedures for Handling Critical Infrastructure Information, Proposed Rule, 6 Code of Federal Regulations (CFR) Part 9 (April 15, 2003); • Freedom of Information Act and Privacy Act Procedures, DHS Interim Final Rule, (January 27, 2003); • Procedures for Handling Critical Infrastructure Information (6 CFR Part 29), published as DHS Interim Final Rule, February 20, 2004, creating the PCII office to protect voluntarily provided information from the private sector; • Executive Order 13231 dealing with critical information protection; • HHS Standards for Privacy of Individually Identifiable Health Information Regulation Text; Security Standards for the Protection of Electronic Protected Health Information; General Administrative Requirements, including Civil Money Penalties; Procedures for Investigations, Imposition of Penalties, and Hearings (45 CFR Parts 160 and 164), December 28, 2000, as amended (May 31, 2002; August 14, 2003; February 20, 2003; and April 17, 2003)); • Economic Espionage Act of 1996 (18 U.S.C. 1831); and • Government Performance and Results Act of 1993 (31 U.S.C. 1115).

Types of Authorities	Laws, Regulations, Executive Orders, and Other Authorities
Developing and Promulgating Plans	• Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458); • Comprehensive Environmental Response, Compensation, and Liability Act of 1980; • Clean Water Act of 1980; • Energy Reorganization Act of 1974; • Project BioShield Act of 2004; • HSPD-3 directing industries to develop their own protective measures (March 11, 2002); • HSPD-7 directing the creation of various infrastructure protection plans (December 17, 2003); • HSPD-8 encouraging greater preparedness on the part of State and local entities against terrorist attacks (December 2003); • PDD-75 establishing a counterintelligence role in identifying and protecting critical national assets; • HHS Concept of Operations Plan (COOP) for Public Health and Medical Emergencies; • DoD, Strategy for Homeland Defense and Civil Support, June 2005; • Public Health Service Act of 1944 (42 U.S.C. 201-300hh-11), as amended; • Social Security Act of 1935 (42 U.S.C. 1320b-5), as amended; • Federal Food, Drug, and Cosmetic Act of 1938 (21 U.S.C. 301, et seq.), as amended; • Executive Order 13347, Individuals With Disabilities in Emergency Preparedness (July 2004); and • The Older Americans Act of 1965 (Public Law 106-501), as amended.
Protecting Critical Infrastructure	• The Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458); • National Strategy for Homeland Security (2002); • National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (2003); • National Response Plan (2006); • Department of Homeland Security Strategic Plan (2004); • Strategic Plan to Combat Bioterrorism and Other Public Health Threats and Emergencies (2003); • Interim National Infrastructure Protection Plan (2005); and • National Strategy to Secure Cyberspace (2004).
Conducting R&D	• National Science and Technology Policy, Organization and Priorities Act of 1976 (Public Law 94-282); • Title VIII, Section 815, of the USA Patriot Act (October 2001); • Cyber Security Research and Development Act of 2002 (Public Law 107-305); • Project BioShield Act of 2004; • National Plan for Research and Development in Support of Critical Infrastructure Protection of 2004; • Public Health Service Act (42 U.S.C. 201-300hh-11); • Social Security Act of 1935 (42 U.S.C. 1320b-5); and • Federal Food, Drug, and Cosmetic Act (21 U.S.C. 301, et seq.)

Types of Authorities	Laws, Regulations, Executive Orders, and Other Authorities
Providing Federal Assistance to State and Local Authorities	• Public Health Threats and Emergencies Act of 2000 (Public Law 106-505); • Robert T. Stafford Disaster Relief and Emergency Assistance Act of 2005 (42 U.S.C. 5121 et seq.); • Public Health Service Act (42 U.S.C. 201-300hh-11); • Social Security Act of 1935 (42 U.S.C. 1320b-5); • Federal Food, Drug, and Cosmetic Act (21 U.S.C. 301, et seq.); • DoD 3025.1, Military Support to Civil Authorities (June 2005); and • National Response Plan (formerly the Federal Radiological Emergency Response Plan).
Protecting Freedom and Privacy	• Freedom of Information Act of 1966 (5 U.S.C. 552), as amended; • Privacy Act of 1974 (5 U.S.C. 552(a)); • Financial Management Act of 1999 (Gramm-Leach-Bliley); • Government Performance and Results Act of 1993 (31 U.S.C. 1115); and • Standards for Privacy of Individually Identifiable Health Information, Final Rule (42 CFR Part 2).
Protecting Workforces	• The Occupational Safety and Health Act of 1970 (Public Law 91-596), in particular, Section 13, Procedures to Counteract Imminent Dangers; and • Executive Order 13347, Individuals with Disabilities in Emergency Preparedness (July 2004).

3.2 State and Local Authorities

Most public health authority is based in the States, typically as an exercise of their police powers.[72] States use this authority in a number of ways to protect public health, including enforcing safety and sanitation codes, conducting inspections, mandating the reporting of certain diseases to State authorities, compelling isolation or quarantine, and licensing healthcare workers and facilities.

Local governments are often responsible for some of these activities, using powers largely derived from delegation of State authority.[73] Most states can declare public emergencies, expanding their powers still further on a temporary basis. States are currently updating their laws for dealing with public health emergencies, using the draft model legislation on emergency health powers, called the Model State Emergency Health Powers Act, which was prepared by the Center for Law and Public Health at Georgetown University and Johns Hopkins University at the request of CDC.[74]

Many public hospitals are owned and operated by special districts and governed by their own locally elected officials, who report to their own constituencies. These local governments that own and operate hospitals are neither Federal, State, nor county agencies, but are elected, independent governmental units. Many have their own ordinance-making authorities.[75]

[72] The term "police powers" is derived from the Tenth Amendment to the Constitution of the United States, which reserves to the States those rights and powers not delegated to the U.S. Government. Historically, these have been interpreted to include authority over the welfare, safety, health, and morals of the public.

[73] See Sarah A. Lister, Specialist in Public Health and Epidemiology, Domestic Social Policy Division, An Overview of the U.S. Public Health System in the Context of Emergency Preparedness, updated March 17, 2005, Congressional Research Service, Library of Congress.

[74] Reflects comments by the HHS Office of the General Counsel in December 2005.

[75] Information provided by SCC members during September 2006.

Appendix 4: Summary of Methods Reviewed

Table	Title
A4-1	Risk Assessment Methodologies for Use in the Electric Utility Industry (Review Draft)
A4-2	Australia/New Zealand Risk Management Guideline
A4-3	Communication, Assessment, and Prioritization Program (CAPP), PNNL Risk Communication Assessment and Prioritization Program
A4-4	American Electric Power Attack Tree Methodology
A4-5	Risk-Assessment Methodology for Dams and Electric Transmission
A4-6	EEI Security Committee Approach to Risk/Vulnerability Assessment
A4-7	Building for Environmental and Economic Sustainability
A4-8	Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability + Shock
A4-9	Hospital Emergency Analysis Tool
A4-10	Security Code of Management Practices for Physical and Cyber Security Activities
A4-11	Information Design Assurance Red Team
A4-12	INFOSEC Assessment Methodology
A4-13	International General Security Risk Assessment Guideline
A4-14	Natural Disaster Mitigation in Drinking Water and Sanitation Systems: Guidelines for Vulnerability Analysis
A4-15	Physical Security Assessment for Department of Veterans Affairs Facilities
A4-16	Project Matrix and Its Function, Service, and Product Evaluation Tool

Table	Title
A4-17	Vulnerability Risk Assessment Program
A4-18	ASME Risk Analysis and Management for Critical Assets Protection
A4-19	Department of Defense Standard Practice for System Safety
A4-20	Balanced Survivability Assessments
A4-21	TAME: Threat Assessment Model for the METEORE System
A4-22	Toward a Secure Systems Engineering Methodology
A4-23	Vulnerability Assessment Methodology for U.S. Chemical Facilities
A4-24	Vulnerability Assessment Survey Program: Overview of Assessment Methodology
A4-25	Wholesale Medical Logistics Readiness Plan
A4-26	Tools, Standards, and Publications for Assessing the Security of Automated Systems Published by the National Institute of Standards and Technology
A4-27	Some Representative Tools, Standards, or Publications for Assessing Automated Systems
A4-28	Selected ISO Standards Related to IT Security

Table A4-1: Risk Assessment Methodologies for Use in the Electric Utility Industry (Review Draft)

Characteristic	Summary Description
Sponsor/Owner	North American Electric Reliability Council.
Reference	Risk-Assessment Working Group of the North American Electric Reliability Council's Critical Infrastructure Protection Committee, *Review Draft: Risk Assessment Methodologies for Use in the Electric Utility Industry*, April 25, 2005.
Purpose	To summarize eight existing risk assessment methodologies to highlight the strengths of each method as applied to the electric utility industry.
Threat Spectrum	Vulnerability, risk, risk reduction, risk management.
Focus	Methodological review of: (1) the Edison Electric institute Security Committee's approach; (2) RAMCAP; (3) Australia/New Zealand Standard for Risk Management; (4) the DOE Vulnerability and Risk Assessment Program; (5) Risk Assessment Methodology for Dams and Risk Assessment Methodology for Transmission; (6) Pacific Northwest National Laboratory Communications Assessment and Prioritization Program; (7) American Electric Power model; and (8) Electric Power Research Institute Security Vulnerability Self-Assessment Guidelines for the Electric Power Institute.

Characteristic	Summary Description
Personnel and/or Implementation Issues	Varies by methodology reviewed. Authors suggest a version they believe captures the most important issues.
Sample	Varies by methodology.
Instrumentation	Varies by methodology.
Method	Varies by methodology.
Analysis	Identifies commonalities among methods, including such steps as: (1) identify and characterize key assets; (2) identify and characterize threats; (3) identify and characterize existing protective and mitigation measures; (4) identify and characterize vulnerabilities; (5) estimate probabilities and consequences; and (6) estimate and assess risk. Points out some weaknesses of each method relative to electric power industry purposes.

Table A4-2: Australia/New Zealand Risk Management Guidelines

Characteristic	Summary Description
Sponsor/Owner	Governments of Australia and New Zealand.
Reference	*Australia/New Zealand Risk Management Guidelines* (AS/NZS 4360:2004), 2004, www.riskmanagement.com.au.
Purpose	To provide standardized risk management guidance for Australian and New Zealand industries, especially the electric power sector.
Threat Spectrum	Risk assessment; risk management.
Focus	Focuses on overall principles, not specific methods, and is intended to be used in nearly any industry in Australia or New Zealand.
Personnel and/or Implementation Issues	Emphasizes need for involvement at all levels of the organization, not just individual analysts.
Sample	None specified.
Instrumentation	None specified.
Method	Describes a five-step framework for risk assessment that includes the following: (1) establish the context; (2) identify the risks; (3) analyze the risks; (4) evaluate the risks; and (5) treat the risks. Devotes considerable attention to the activities recommended under each of these headings.
Analysis	Highlights the need for iterative processing of risk assessment information and continuing involvement of top management in the overall risk assessment process. Does not discuss once-in-a-lifetime events, and devotes little attention to risk control measures.

Table A4-3: PNNL Risk Communication Assessment and Prioritization Program

Characteristic	Summary Description
Sponsor/Owner	Western Area Power Administration (United States).
Reference	PNNL *Risk Communication Assessment and Prioritization Program (CAPP)*, no date. Brown, Bowen, DiMassa, Glantz, Roybal, Ortiz, *Environmental Risk Communication, Assessment, and Prioritization Program (CAPP)*, Version 1.1, User's Guide, PNNL-11338, Pacific Northwest National Laboratory, Richland, Washington, http://mepas.pnl.gov/earth/capp.html.
Purpose	To provide a simple, easy-to-implement risk assessment and management tool for dealing with environmental issues.
Threat Spectrum	Risk management.
Focus	Primarily focused on environmental risk assessments. Versions of CAPP have also been developed for prioritizing the allocation of funds for environmental restoration projects at DOE sites.
Personnel and/or Implementation Issues	Not discussed.
Sample	Not discussed.
Instrumentation	Two instruments include: (1) the Qualitative Issue Characterization (QuIC) used to gather and record information on issues, their potential impacts, and the organization's ability to address these issues and mitigate negative impacts; and (2) the SEQUEL analytic tool, which involves the evaluation of risks and the evaluation of the organization's ability to manage risk. Both instruments are combined in a software package called CAPP.
Method	Two basic elements include a qualitative tool to support both information gathering and risk screening, and a semi-quantitative tool for evaluating risk levels, the organization's ability to manage that risk, and exploring various risk management options.
Analysis	The CAPP approach focuses on identifying issues, collecting information on these issues, the organization's current ability to address these issues, conducting simple semi-quantitative assessments of risk and ability to manage risk, and improving risk management.

Table A4-4: American Electric Power Attack Tree Methodology

Characteristic	Summary Description
Sponsor/Owner	The American Electric Power Institute.
Reference	AEP, *American Electric Power Attack Tree Methodology, no date. Also see NASA, Fault Tree Handbook with Aerospace Applications,* August 2002, www.hq.nasa.gov/office/doceq/doctree/fthb.pdf.
Purpose	To provide a tool for dynamically evaluating business risk associated with both cyber and physical threats to electrical power facilities.
Threat Spectrum	Threats, vulnerabilities, needs for mitigation.
Focus	Both physical and cyber threats to facilities and steps that must be taken to mitigate these threats.
Personnel and/or Implementation Issues	None identified.
Sample	None identified.
Instrumentation	Analytical threat and vulnerability trees.
Method	Threat (or fault) trees are used to determine whether the conditions necessary for a threat to be realized exist and are unmitigated. A threat tree consists of threat outcomes (e.g., long-term service disruption to a large area), where pre-existing conditions must exist for an adversary to realize the threat. This information is combined with intelligence about adversaries to create an attack tree that helps identify feasible attack modes.
Analysis	The methodology has a long history in many fields where one must examine threat capabilities in conjunction with possible vulnerabilities. The impact of a threat can be calculated quickly from the attack tree. This impact, in turn, can be used to justify expenditures on mitigation strategies.

Table A4-5: Risk-Assessment Methodology for Dams and Electric Transmission

Characteristic	Summary Description
Sponsor/Owner	The Interagency Forum for Infrastructure Protection (IFIP), including the U.S. Army Corps of Engineers, the U.S. Bureau of Reclamation, the Tennessee Valley Authority, the Bonneville Power Administration, the Lawrence Livermore National Laboratory, the FBI, the Western Area Power Administration, and Sandia National Laboratories.
Reference	*Risk-Assessment Methodology for Dams and Electric Transmission*, no date. The RAM-DSM and RAM-TSM Field Manuals, Training Guide, Fault Trees, and Exercise Workbook available from the IFIP.
Purpose	The RAM-DSM and RAM-TSM models have been developed to evaluate security risks for dams and transmission systems, respectively.
Threat Spectrum	Threats, risks, and risk mitigation.
Focus	This methodology helps define the likelihood of an attack, the consequences of a successful attack, and the effectiveness of physical protection systems in preventing an attack.
Personnel and/or Implementation Issues	None specified.
Sample	Oriented toward the entire dam and supporting facilities.
Instrumentation	The risk assessment process for RAM is embodied in the following risk equation: (Likelihood of Attack)* (Consequence)* (1-System Effectiveness) = Risk.
Method	Identifies and analyzes characteristics of each facility, including the mission(s) of the substation and control center; the undesired events that would prevent mission(s) success; the critical assets that must be protected to prevent these undesired events from occurring; the potential adversaries and their characteristics; the credible threats to the power system or individual facility; the level of risk that can be tolerated at the facility; the optimal use of available techniques for security upgrades; the consequence mitigation options; the risk reduction alternatives; and the operational and cost impacts of these alternatives.
Analysis	The RAM process has four major elements: threat assessment (likelihood of attack), consequence assessment, assessment of system effectiveness, and risk assessment. Each element addresses a separate component of the risk equation.

Table A4-6: EEI Security Committee Approach to Risk/Vulnerability Assessment

Characteristic	Summary Description
Sponsor/Owner	DOE, North American Electric Reliability Council.
Source	EEI Security Committee, *The EEI Security Committee Approach to Risk/Vulnerability Assessment*, no date. North American Electric Reliability Council (NERC), *Security Guidelines for the Energy Sector: Vulnerability and Risk Assessment, Version 1.0*, www.esisac.com/publicdocs/Guides/V1.
Purpose	To provide a practical and straightforward approach to assessing the nature of risk and vulnerability to an entity's critical facilities and systems.
Threat Spectrum	Risk, vulnerability, mitigation.
Focus	Primarily electrical power and natural gas facilities.
Personnel and/or Implementation Issues	None identified.
Sample	None identified.
Instrumentation	Top-down set of principles, not a detailed methodology with instrumentation.
Method	The method has six steps: (1) identify assets and loss impact; (2) identify and characterize the threat; (3) identify vulnerabilities; (4) identify mitigation measures; (5) assess risk and determine protection priorities; and (6) document, implement, and validate the process.
Analysis	This approach can be utilized by a broad range of entities, ranging from large entities operating in multiple states to very small entities with limited security resources.

Table A4-7: Building for Environmental and Economic Sustainability

Characteristic	Summary Description
Sponsor/Owner	National Institute of Standards and Technology (NIST).
Reference	Biomass Research and Development Initiative Web site, www.bioproducts-bioenergy.gov/office.html. See NISTIR 6806, *Project Oriented Life-Cycle Costing Workshop for Energy Conservation in Buildings*, Fuller, Rushing, and Meyer.
Purpose	To predict and measure technologies and technical advances to improve the life-cycle quality of constructed facilities. See description of the Building for Environmental and Economic Sustainability (BEES) instrument and software for more details).
Threat Spectrum	Life-cycle vulnerability, impact.
Focus	Building products (i.e., technologies and technical aspects of constructed facilities).
Personnel and/or Implementation Issues	None specified.
Sample	None specified.
Instrumentation	BEES software is used to measure the environmental performance of building products using the internationally standardized and science-based Life-Cycle Assessment method. All stages of the life of a product are analyzed (i.e., raw material acquisition, manufacture, transportation, installation, use, and recycling and waste management).
Methodology	None specified other than BEES and related tools/analyses.
Analysis	Environmental impact analysis measures the product's impact on global warming, acidification, indoor air quality, resource depletion, and solid waste. Economic performance is analyzed using the American Society for Testing and Materials standard for Multi-Attribute Decision Analysis, which includes costs of initial investment, replacement, operation, maintenance and repair, and disposal. BEES combines the environmental and economic performance scores into an overall performance score.

Table A4-8: Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability + Shock

Characteristic	Summary Description
Sponsor/Owner	Department of Agriculture.
Reference	*CARVER Plus Shock Method for Food Sector Vulnerability Assessments*, privileged, unclassified report, August 17, 2005. PowerPoint Briefing: NERC CI/KR Protection Security Workshop: Meeting the Security Challenge, no date.
Purpose	An offensive targeting prioritization tool that can be adapted to various sectors to assess the vulnerabilities within a system or infrastructure to an attack. It prompts the user to think like an attacker by identifying the most attractive targets for attack.
Threat Spectrum	Vulnerability, impact, threat, risk.
Focus	Can be applied across industries and systems.
Personnel and/or Implementation Issues	A team of subject matter experts should be assembled to conduct the assessment.
Sample	Farm-to-table supply chains are mentioned in the Food and Agriculture Sector Report, August 17, 2005.
Instrumentation	Instruments include: (1) worksheet for calculating criticality; (2) summary sheet totaling scores for nodes across attributes; and (3) scales developed for each of seven attributes, ranked from 1-10. Conditions associated with lower attractiveness (or lower vulnerability) are assigned lower values (e.g., 1 or 2). Conditions associated with higher attractiveness (or higher vulnerability) are assigned higher values (e.g., 9 or 10).
Methodology	Step 1: Establish Parameters; Step 2: Assemble Experts; Step 3: Detail System Under Evaluation (flowchart, etc.); Step 4: Assign Scores; and Step 5: Apply What Has Been Learned.
Analysis	Step 4: To rank and score each of the seven CARVER + Shock attributes and calculate an overall score for that node is the most important. The rationale for a particular consensus score should be documented.

Table A4-9: Hospital Emergency Analysis Tool

Characteristic	Summary Description
Sponsor/Owner	U.S. Navy. DVATEX is a partnership of the Navy Medicine's Office of Homeland Security, EAI, Inc., and U.S. Navy Medical Treatment Facilities (MTFs).
Reference	PowerPoint Briefing: Disaster Preparedness, Vulnerability Analysis, Training and Exercise (DVATEX) Program. Lieutenant Mark R. Lauda, Asst. Head, DVATEX Program, Navy Medicine, Office of Homeland Security, no date.
Purpose	Strengthen emergency preparedness capabilities in all U.S. Navy medicine hospitals and clinic commands. HEAT is designed to measure critical factors that reflect the level of emergency preparedness; IT can compare a hospital with itself over time to evaluate progress toward reducing vulnerability.
Threat Spectrum	Vulnerability.
Focus	U.S. Navy hospitals and clinical commands.
Personnel and/or Implementation Issues	Employs a multidiscipline team that includes: • Emergency/disaster medicine physicians; • Emergency nurses; • Healthcare executives; • Emergency medical services experts; and • Facilities engineers.
Sample	None specified.
Instrumentation	Standard evaluation scale (1-100).
Methodology	Major steps include: • Survey hospital; • Examine records; and • Conduct interviews.
Analysis	All major steps (e.g., survey the hospital, examine records, and conduct interviews) employ structured forms and multidisciplinary teams.

Table A4-10: Security Code of Management Practices for Physical and Cyber Security Activities

Characteristic	Summary Description
Sponsor/Owner	American Chemistry Council.
Reference	American Chemistry Council, *Implementation Resource Guide for Responsible Care Security Code of Management Practices: Cyber Security Activities*, May 2, 2003.

Characteristic	Summary Description
Purpose	Two major purposes: (1) to help protect people, property, products, processes, information, and information systems by enhancing security, including security against potential terrorist attack, throughout the chemical industry value chain; and (2) to help companies achieve continual improvement in security performance using a risk-based approach to identify, assess, and address vulnerabilities; prevent or mitigate incidents; enhance training and response capabilities; and enable collaborative business operations.
Threat Spectrum	Threats, vulnerabilities, impact.
Focus	People, property, products, processes, information, and information systems.
Personnel and/or Implementation Issues	A team of company experts drawn from distribution; logistics; customer support; marketing; sales; risk; security; legal; corporate; site/facility functions; all aspects of the company digital systems; and environmental, health, and safety. One team may implement the entire code with subsets of the team responsible for different security aspects (e.g., site, value chain, cyber security).
Sample	None mentioned.
Instrumentation	For Management Practice #2, several cyber security vulnerability methodologies may be considered. See report for details.
Methodology and/or Data Collection Process	A management system approach and many of the security code practices overlap one another. The process includes the following: • Develop a thorough understanding of the Security Code; • Identify company's current cyber security activities and compare to Security Code management practices; • Develop action list of priority items to implement for each practice; and • Develop an implementation plan. Management Practices (1-13) 1. Leadership Commitment 2. Analysis of Threats, Vulnerabilities, and Consequences 3. Implementation of Security Measures 4. Information Security and Cyber Security 5. Documentation 6. Training, Drills, and Guidance 7. Communications, Dialogue, and Information Exchange 8. Response to Security Threats 9. Response to Security Incidents 10. Audits 11. Third-Party Verifications 12. Management of Change 13. Continuous Improvement
Analysis	High-level risk assessment, analysis of threats, and risk mitigation. No specific analysis is mentioned.

Table A4-11: Information Design Assurance Red Team

Characteristic	Summary Description
Sponsor/Owner	Sandia National Laboratories.
Reference	See Web site www.sandia.gov/idart/index.html.
Purpose	To improve the security of high-consequence information systems critical to national security by providing independent assessments of critical information systems that are performed from an adversary point-of-view, are consequence-based, and are systems-oriented.
Threat Spectrum	Vulnerability, threat, impact.
Focus	Information operations.
Personnel and/or Implementation Issues	Red Teams customized exclusively for the project, using resources within the Information Assurance and Survivability Organization and resources throughout Sandia National Laboratories, as necessary, to build Red Teams. Some useful specializations include: cryptographic research, advanced networked systems survivability, R&D of agent-based systems, physical security, operations support, and weapons.
Sample	None specified.
Instrumentation	None specified.
Methodology	The methodology has five phases: • Phase I: Planning Phase: Understand the problem and threat space of concern; • Phase II: Data Collection Phase: Open source and customer-provided information; • Phase III: Characterization Phase: Based on several aspects for identifying and understanding single points of failure, high-value nodes, and security controls that can be circumvented; • Phase IV: Analysis Phase: Weaknesses, vulnerabilities to the depth and breadth specified by the customer; and • Phase V: Report Phase: Demonstrations, attacks, or experiments.
Analysis	See Analysis Phase.

Table A4-12: INFOSEC Assessment Methodology

Characteristic	Summary Description
Sponsor/Owner	National Security Agency (NSA), INFOSEC Assurance Training and Rating Program (IATRP).
Reference	IAM home page at www.iatrp.com/iam.cfm.
Purpose	• Conduct a high-level review of the Information Security (INFOSEC) posture of operational system(s) to identify potential vulnerabilities. • Serves as the first step in the vulnerability discovery triad to provide initial information for risk management decisions and the focus of further INFOSEC analysis (e.g., use of other triad services such as evaluations or Red Teams). • Recommendations are provided for the elimination or mitigation of vulnerabilities.
Threat Spectrum	Vulnerability, threat, impact.

Characteristic	Summary Description
Focus	Policy, procedures, and information flow.
Personnel and/or Implementation Issues	Analysis and report generation are completed 45 to 60 days after Phase II.
Sample	None specified.
Instrumentation	During Phase II there is a hands-on process, cooperative testing, diagnostic tools, and penetration tools.
Methodology and/or Data Collection Process	• Phase I: On-site customer coordination with information criticality analysis and identification of customer concerns (using interviews, documentation review, and system demonstrations to uncover information in 18 baseline INFOSEC categories). Categorize and define value of information, identify systems and boundaries. • Phase II: Documented INFOSEC Assessment Plan. • Phase III: Documented final report of findings and recommendations.
Analysis	None specified.

Table A4-13: International General Security Risk Assessment Guidelines

Characteristic	Summary Description
Sponsor/Owner	ASIS International, Alexandria, Virginia.
Reference	Web site guidelines at www.asisonline.org.
Purpose	To create a methodology for security professionals by which security risks at a specific location can be identified and communicated, along with appropriate solutions.
Threat Spectrum	Assessment, risk, threat, vulnerability.
Focus	Any environment where people and/or assets are at risk for security-related incidents or events that may result in deaths, injury, or loss of an asset.
Personnel and/or Implementation Issues	Security professionals.
Sample	None specified.
Instrumentation	None specified.
Methodology	Seven-step process includes the following: • Identify assets; • Specify loss events; • Determine frequency of events; • Determine impact of events; • Identify options to mitigate; • Assess feasibility of options; and • Conduct cost-benefit analysis.

Characteristic	Summary Description
Analysis	• Conduct cost-benefit analysis to determine actual costs of program implementation and weigh those costs against the impact of loss, financial or otherwise. • Calculate probability and criticality. • Create risk matrix. • Make probability ratings.

Table A4-14: Natural Disaster Mitigation in Drinking Water and Sanitation Systems: Guidelines for Vulnerability Analysis

Characteristic	Summary Description
Sponsor/Owner	Pan-American Health Organization (PAHO).
Reference	Slide Presentation: Disaster Mitigation in Drinking Water and Sanitation Systems, 2002.
Purpose	To promote and facilitate the incorporation of disaster mitigation measures in drinking water and sanitation infrastructures, reducing the damage caused by natural disasters and ensuring the continuity of key services in their aftermath.
Threat Spectrum	Vulnerability, risk.
Site Type	Drinking water and sanitation systems.
Personnel and/or Implementation Issues	None specified.
Sample	None specified.
Instrumentation	None specified.
Methodology	Vulnerability assessment with the following steps: • Define criteria for reducing the risk; • Identify risks either quantitatively or qualitatively; • Identify operation/management standards and available resources; • Conduct technical studies to assess potential damage; and • Design and implement mitigation, preparedness, and response measures.
Analysis	Successful completion of methodology produces risk maps that depict risks by severity.

NOTE: Several vulnerability assessment tools are available to help water utilities evaluate their susceptibility to potential threats and identify corrective actions to reduce or mitigate the risk of serious consequences from vandalism, insider sabotage, or terrorist attack. For further information about available tools, see http://cfpub.epa.gov/safewater/watersecurity/home.cfm?program_id=11.

Table A4-15: Physical Security Assessment for Department of Veterans Affairs Facilities

Characteristic	Summary Description
Sponsor/Owner	Department of Veterans Affairs (VA), conducted by the National Institute of Building Sciences (NIBS) Task Force.
Reference	*Physical Security Assessment for Department of Veterans Affairs Facilities: Recommendations of the NIBS Task Group,* September 6, 2002.
Purpose	Provide an implementation plan for VA to systematically assess the vulnerability of its facilities and provide mitigation solutions.
Threat Spectrum	Vulnerability, impact, threat, risk.
Focus	Deals with physical threats only. Assesses site; architectural; structural; building envelope; utility/ mechanical/plumbing/ electrical systems; and security master plan.
Personnel and/or Implementation Issues	Recommends team with high levels of expertise in architecture; civil/structural engineering; mechanical/ electrical engineering; security operations/systems engineering; chemical, biological, and radiological specialties; and cost estimation.
Sample	All VA facilities.
Instrumentation	Physical Security Facility Assessment Checklist provided in report.
Methodology	Three phases: • Phase I: Define the criticality of VA facilities, called the Minimum Critical Infrastructure (MCI); • Phase II: Identify vulnerabilities of VA's critical facilities; and • Phase III: Assess and analyze vulnerable VA facilities and identify remedial actions.
Analysis	Essentially a life-cycle analysis for physical facilities.

Table A4-16: Project Matrix and Its Function, Service, and Product Evaluation Tool

Characteristic	Summary Description
Sponsor/Owner	DHS, Office of Infrastructure Protection Division.
Reference	HHS CI/KR Protection Plan.
Purpose	Three purposes: (1) objectively determine which HHS missions, assets, and functions are nationally critical according to criteria established by HSPD-7; (2) map the interdependencies among the assets and links that are essential to perform or provide their functions and services; and (3) understand relationships with national infrastructures, water, power, and telecommunications.
Threat Spectrum	Risks to national or economic security and risks to public health and safety.
Focus	Major HHS facilities and systems in the post HSPD-7 period.
Personnel and/or Implementation Issues	Employs rankings by Federal officials associated with their respective programs together with a data-gathering activity.
Sample	Scheduled are Operating Divisions and HHS laboratories.
Instrumentation	The Function, Service, and Product Evaluation Tool (FSPET) as modified to take new requirements posed by HSPD-7 into account.
Methodology	Employs the DHS risk management framework using six major steps: • Identify security requirements; • Collect and analyze physical security data; • Identify physical security threats; • Identify physical security vulnerabilities; • Formulate security risks; and • Develop assessment report.
Analysis	Incorporates the CI/KR protection requirements levied by HSPD-7.

Table A4-17: Vulnerability Risk Assessment Program

Characteristic	Summary Description
Sponsor/Owner	North American Electric Reliability Council (NERC).
Reference	NERC, *Security Guidelines for the Energy Sector: Vulnerability and Risk Assessment,* Version 1.0, 2002.
Purpose	To help energy sector organizations identify and understand the threats to, and vulnerabilities of, their infrastructures and to stimulate actions to mitigate significant problems.
Threat Spectrum	Vulnerabilities, risks, risk mitigation.
Focus	Encompasses pre-assessment, assessment, and post-assessment phases of risk analysis.
Personnel and/or Implementation Issues	Not specified in detail, but emphasizes engaging the full range of knowledgeable staff in the process.
Sample	Not specified in detail.
Instrumentation	Not specified in detail.
Methodology	Four main analytical steps include: (1) identify all critical vulnerabilities, both physical and cyber, and develop appropriate response options; (2) identify and rank all key assets from a security perspective; (3) develop the business case for making security investments and organizational changes that will enhance security; and (4) enhance awareness and make security an integral part of the business strategy.
Analysis	The VRAP pre-assessment calls for: (1) identifying the assessment objectives and measures of success; (2) specifying the elements of the methodology that will be included in the assessment; (3) engaging knowledgeable personnel and ensuring their access to resources and information; (4) deciding what type of assessment (internal, facilitated, external, or hybrid) to conduct; and (5) developing an assessment schedule. The post-assessment phase calls for: (1) prioritizing assessment recommendations, (2) developing an action plan, (3) capturing lessons learned and best practices, and (4) conducting training.

Table A4-18: ASME Risk Analysis and Management for Critical Assets Protection

Characteristic	Summary Description
Sponsor/Owner	DHS and the American Society of Mechanical Engineers (ASME).
Reference	PowerPoint Briefing: ASME, Critical Assets Protection Initiative ASME Homeland Security: ASME Risk Analysis and Management for Critical Assets Protection (RAMCAP) Methodology Document, September 17, 2004.
Purpose	To provide a common framework for homeland security risk analysis decision-making (i.e., common terminology, metrics for comparing risks across sectors, basis for reporting results and informing resource allocation decisions), and provide a basis for comparing risks across sectors.
Threat Spectrum	Vulnerability, threat, risk, impact.
Focus	RAMCAP is most applicable to the following nine sectors: • Commercial nuclear power plants; • Commercial nuclear spent fuel storage facilities; • Chemical plants; • Petroleum refineries; • Liquefied natural gas (LNG) storage facilities; • Subway systems (including bridges and tunnels); • Railroad systems (including bridges and tunnels); • Highway systems (including bridges and tunnels); and • Power generation and transmission facilities.
Personnel and/or Implementation Issues	Team recommendations are not provided in this report.
Sample	None specified. (See RAMCAP full document for more details.)
Instrumentation	None specified. (See RAMCAP full document for more details.)

Characteristic	Summary Description
Methodology	RAMCAP methodology recommends the following 11 steps: 1. Prepare for study (define objectives and scope, form team, identify assets and threats); 2. Perform screening analysis (identify available information, select a screening method and assets for analysis); 3. Analyze threats (define tactical threats, determine frequency ranges of credible threats); 4. Analyze vulnerabilities (determine conditional probabilities of credible threats); 5. Analyze consequences (determine consequences resulting from vulnerabilities); 6. Collect data and opinion; 7. Analyze risks (compute scenario risks with uncertainties; aggregate risks); 8. Identify action strategies (identify countermeasures/mitigations; assess costs); 9. Analyze benefits and costs (assess residual risks, benefits, and costs; make informed decisions); 10. Perform risk analysis for multiple sectors (analyze groups of sectors focusing on national impacts); and 11. Perform sector regional risk analysis (analyze groups of assets).
Analysis	Basic Risk Equation 1: $R_{ai} = F_{ai}$ x *(Vulnerability) ij x (Consequences) ij* Where: R_{ai} = annual economic risk for a given threat *I*; F_{ai} = annual frequency of an adversary attacking a critical asset using a specific type of threat, *I*; *Vulnerability* = conditional probability that a specific failure mode, *j*, will occur, assuming that the assumed threat, *i*, has occurred; and *Consequences* = total measure of consequences of failure for threat *i*, failing in mode *j*. Basic Risk Equation 2: $R_{ijk} = F_{ai}P_{fij}P_{cijk}C_{cijk}$; Where: R_{ijk} = economic risk; F_{ai} = annual frequency of an adversary attacking a critical asset using a specific type of threat; P_{cijk} = combination of the probability ranges at each node of the event tree starting at the node, after the node where Pfij is defined; P_{fij} = conditional probability of failure mode j due to threat I; F_{ai} = annual frequency of an adversary attacking a critical asset using a specific type of threat, I; and If F_{ai} is set to 1.0, then the calculated risk is termed a “conditional threat risk.”

Table A4-19: DoD Standard Practice for System Safety

Characteristic	Summary Description
Sponsor/Owner	Department of Defense.
Reference	*Department of Defense Standard Practice for System Safety* MIL-STD-882D, February 10, 2000.
Purpose	To achieve acceptable risk associated with mishaps (i.e., unplanned event or series of events resulting in death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment) through a systematic approach employing hazard analysis, risk assessment, and risk management.
Threat Spectrum	Vulnerability, risk, threat, impact.
Focus	Useful for all agencies within DoD. Technology development by design for DoD systems, subsystems, equipment, facilities, and their interfaces and operation.
Personnel and/or Implementation Issues	None specified.
Sample	None specified.
Instrumentation	Standardization Document Improvement Proposal Form (for post-assessment).
Methodology and/or Data Collection Process	General requirements include the following: • Document the system safety approach; • Identify hazards; • Assess mishap risks; • Identify mishap risk mitigation measures; • Reduce mishap risk to an acceptable level; • Verify mishap risk reduction; • Review hazards and accept residual mishap risk by the appropriate authority; and • Track hazards, their closures, and residual mishap risk.
Analysis	Commonly used approaches for assessing mishap risks can be found in the *Defense Acquisition Desk Book* and in the System Safety Society's *System Safety Analysis Handbook*.

Table A4-20: Balanced Survivability Assessments

Characteristic	Summary Description
Sponsor/Owner	DoD, Defense Threat Reduction Agency (DTRA).
Reference	PowerPoint Briefing: Balanced Survivability Assessment, Commercial Entity Initiative, D.R. Lewis, Chief, BSA Branch, DTRA, July 10, 2003.
Purpose	Integrated, multi-disciplined, performance-based assessments to identify the vulnerabilities of critical missions and recommend ways to mitigate them.
Threat Spectrum	Broad spectrum of threats, vulnerability.
Focus	• System architecture/security safety; • Support/operational practices/systems vulnerabilities; and • Identify single-point vulnerability.
Personnel and/or Implementation Issues	Recommends team matched to site needs (~15 members), and approximately 2 to 3 weeks on site.
Sample	Within DoD, approximately 30 Balanced Survivability Assessments (BSAs) are made per year.
Instrumentation	None specified.
Methodology	Methodology contains the following elements: • On-site observations; • Documentation review; • Interviews; • Open sources; • Threat application ; and • Vulnerability analysis. Final report usually available within 60 to 90 days after the out-briefing. The final report can include recommendations, additional briefings to leadership as requested, continuing assistance, and lessons learned.
Analysis	Single-point vulnerability analysis.

Table A4-21: TAME: Threat Assessment Model for the METEORE System

Characteristic	Summary Description
Sponsor/Owner	University of Glamorgan, School of Computing, Wales, United Kingdom
Source	Vidalis and Blyth, TAME: *A Threat Assessment Model for the METEORE System*, School of Computing Technical Report CS-02-5, October 2002.
Purpose	To provide a method for the assessment and analysis of threat and vulnerabilities within the context of security risk management.
Threat Spectrum	Vulnerability, threat, impact.
Focus	Software vulnerabilities (specific to technologies and processes involved in electronic payment systems).
Personnel and/or Implementation Issues	None specified.
Methodology	Scope: • Business analysis (goals, processes, and environment); • Stakeholder identification (management, users, and developers); • System boundaries identification; and • Threat agent identification and selection. Scenario Construction and Modeling: • Scenario generation; • System modeling; and • Asset identification. Threat Agent and Vulnerability Analysis: • Vulnerability type identification and selection; • Vulnerability complexity calculation; • Threat agent preference structuring; and • Threat agent capabilities. Evaluation: • Stakeholder evaluation; • Scenario selection and conflict resolution; • Threat impact analysis; and • Threat statement generation.
Sample	Developed for performing the security audit of the METEORE prototype micro-payment systems (by NT Systems, Banca Antonveneta, COSI, Business Architects, TIM, and TILab).
Instrumentation	None specified.
Analysis	Specific procedures not discussed.

Table A4-22: Toward a Secure Systems Engineering Methodology

Characteristic	Summary Description
Sponsor/Owner	Interdisciplinary working group sponsored by the National Security Agency (NSA).
Reference	Salter, Saydjari, Schneier, Wallner, *Toward a Secure Systems Engineering Methodology*, NSA Working Group, no date.
Purpose	Not to "penetrate and patch" a system, but rather to discover the sources of system weaknesses and to uncover reasonable design strategies to create stronger systems.
Threat Spectrum	Vulnerability, threat, impact.
Focus	High-level information systems (technologies and processes).
Personnel and/or Implementation Issues	• System engineer to construct the most cost-effective set of countermeasures. • Evaluator to systematically find residual vulnerabilities and rationally assess their residual risk.
Sample	Scenarios included sensitive phone calls and secure e-mail.
Instrumentation	Attack tree software (unspecified).
Methodology	• **Adversary Models:** Characterize adversaries' resources, access, risk tolerance, and objectives. • **Vulnerability Models:** Describe the totality of the vulnerability landscape (i.e., life cycle, physical security, trust model, rational responses to the landscape). • **Attack Tree Models:** Attack trees identifying weak spots, nodes, risk, access, cost to attacker, countermeasures, countermeasures for most exploitable nodes, ranked countermeasures based on five attributes.
Analysis	Attack tree model. See methodology section of the article for details.

Table A4-23: Vulnerability Assessment Methodology for U.S. Chemical Facilities

Characteristic	Summary Description
Sponsor/Owner	DOJ, Office of Justice Programs, and Sandia National Laboratories.
Reference	*A Method to Assess the Vulnerability of U.S. Chemical Facilities, Final Report*, November 2002.
Purpose	To identify and assess potential security threats, risks, and vulnerabilities, and guide the chemical facilities industry in making security improvements.
Threat Spectrum	Threats, risks, vulnerability.
Focus	Chemical facilities.
Personnel and/or Implementation Issues	Team requires a facilitator/corporate manager; other team members unspecified.
Sample	None specified.
Instrumentation	• Facility characterization matrix. • Process control flow diagram. • Form for analysis of operating activities. • Risk-level summary.
Methodology	Methodology contains the following elements: • Screening for the need for a vulnerability assessment; • Defining the project; • Characterizing the facility; • Deriving severity levels; • Assessing threats; • Prioritizing threats; • Preparing for the site analysis; • Surveying the site; • Analyzing the system's effectiveness; • Analyzing risks; • Making recommendations for risk reduction; and • Preparing final report.
Analysis	Risk Analysis defined as a function of: S = Severity of consequences of an event (see Section 4 of report); L_A = Likelihood of adversary attack (see Section 5); L_S = Likelihood of adversary attack and severity of consequences of an event (see Section 6); and L_{AS} = Likelihood of adversary success in causing a catastrophic event (see Section 9).

Table A4-24: Vulnerability Assessment Survey Program: Overview of Assessment Methodology

Characteristic	Summary Description
Sponsor/Owner	DOE, Office of Energy Assurance (OEA).
Reference	*Vulnerability Assessment and Survey Program: Overview of Assessment Methodology*, September 28, 2001.
Purpose	To develop and implement a vulnerability awareness and education program, and enhance the security of the energy infrastructure, as directed by Presidential Decision Directive 63 (PDD-63).
Threat Spectrum	Vulnerability, threat, impact
Focus	Physical and cyber components of electric power, oil, and natural gas infrastructures; the interdependencies among these components; and the interdependencies with the other critical national infrastructures.
Personnel and/or Implementation Issues	• Internal (in-house technical and organizational expertise). • Facilitated (in-house technical experts guided by an outside facilitator). • External (external assessment team, such as the OEA national laboratory vulnerability assessment team). • Hybrid (partly internal staff and partly external experts).
Sample	Eleven voluntary assessments focused on the electric power industry.
Instrumentation	None specified.
Methodology	Pre-assessment: • Define objectives and scope; • Establish information protection procedures; and • Identify and rank critical assets. Assessment: • Analyze network architecture; • Assess threat environment; • Conduct penetration testing; • Assess physical security; • Conduct physical asset analysis; • Assess operations security; • Examine policies and procedures; • Conduct impact analysis; • Assess infrastructure interdependencies; and • Conduct risk characterization. Post-Assessment: • Prioritize recommendations; • Develop action plan; • Capture lessons learned and best practices; and • Conduct training.
Analysis	Physical asset analysis, impact analysis.

Table A4-25: Wholesale Medical Logistics Readiness Plan

Characteristic	Summary Description
Sponsor/Owner	Defense Logistics Agency.
Reference	INS, Inc., *Wholesale Medical Logistics Readiness Plan by the Defense Logistics Agency,* Defense Supply Center Philadelphia. (fifth edition, first printing), February 2004.
Purpose	To meet "customer response and combat readiness" objectives that include putting in place contracts, business rules, and agreements to rapidly acquire the full spectrum of medical supplies and equipment using a multitude of supply sources.
Threat Spectrum	Vulnerability, impact.
Site Type	Designed to meet medical logistics needs of Army, Air Force, Navy, and Marine Corps.
Personnel and/or Implementation Issues	None specified.
Sample	Army, Air Force, Navy, and Marine Corps process their services' requirements biannually. Healthcare industry, manufacturers, and distributors are surveyed for production data and products.
Instrumentation	Industrial Preparedness Planning (IPP) Assessment Survey (for wholesale level) online, desktop, or traditional paper survey. Site visits are conducted to clarify survey.
Methodology	IPP survey results and data reside at the Defense Supply Center, Philadelphia, in the Readiness Management Application (RMA). The Medical Contingency File (MCF) consolidates 60-day updates of time-phased wartime requirements from all four services (Army, Air Force, Navy, and Marine Corps).
Analysis	Supply chain vulnerabilities and risks.

Table A4-26: Tools, Standards, and Publications for Assessing the Security of Automated Systems Published by the National Institute of Standards and Technology

Tool, Standard, or Publication*	Name	Date	Purpose
NIST Special Publication (SP) 800-12	An Introduction to Computer Security: The NIST Handbook	10/1995	This handbook provides assistance in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. It illustrates the benefits of security controls, the major techniques or approaches for each control, and important related considerations.
NIST SP 800-18	Guide for Developing Security Plans for Information Technology Systems	12/1998	The objective of system security planning is to improve protection of IT resources. All Federal systems have some level of sensitivity and require protection as part of good management practices. The protection of a system must be documented in a system security plan. The completion of system security plans is a requirement of the OMB Circular A-130, Management of Federal Information Resources, Appendix III, "Security of Federal Automated Information Resources," and Public Law 100-235, Computer Security Act of 1987.
NIST SP 800-26	Security Self-Assessment Guide for Information Technology Systems	11/2001	Self-assessments provide a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. This self-assessment guide utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. The guide does not establish new security requirements. The control objectives and techniques are abstracted directly from long-standing requirements found in statute, policy, and guidance on security.
NIST SP 800-30	Risk Management Guide for Information Technology Systems	7/2002	Risk is the net negative impact of the exploitation of vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. This guide provides a foundation for the development of an effective risk management program, containing the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems.
NIST SP 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems	5/2004	This publication provides guidelines for the security certification and accreditation of information systems supporting the executive agencies of the Federal Government. The guidelines have been developed to help achieve more secure information systems within the Federal Government by enabling more consistent, comparable, and repeatable assessments of security controls in Federal information systems; promoting a better understanding of agency-related mission risks resulting from the operation of information systems; and creating more complete, reliable, and trustworthy information for authorizing officials to make informed security accreditation decisions.

Tool, Standard, or Publication*	Name	Date	Purpose
NIST SP 800-47	Security Guide for Interconnecting Information Technology	8/2002	This guide deals with planning, establishing, maintaining, and terminating interconnections between information technology systems that are owned and operated by different organizations. A system interconnection is defined as the direct connection of two or more IT systems for the purpose of sharing data and other information resources. This document describes various benefits of interconnecting IT systems, identifies the basic components of an interconnection, identifies methods and levels of interconnectivity, and discusses potential security risks associated with an interconnection.
NIST SP 800-50	Building an Information Technology Security Awareness and Training Program	10/2003	This publication provides guidance for building an effective IT security program. A strong IT security program cannot be put in place without significant attention given to training agency IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure IT resources. NIST makes recommendations for creating the necessary security awareness.
NIST SP 800-53, Revision 1	Recommended Security Controls for Federal Information Systems	12/2005	Security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Three questions are important: (1) what security controls are needed to adequately protect the information systems that support the operations and assets of the organization?; (2) have security controls been implemented or is there a realistic plan for their implementation?; and (3) what is the desired or required level of assurance that the security controls are effective? This publication explores these questions.
NIST Draft SP 800-53A	Guide for Assessing the Security Controls in Federal Information Systems	4/2006	Security controls must be assessed to determine their overall effectiveness as it relates to protecting the confidentiality, integrity, and availability of an information system Assessing controls ensures that they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Security control assessments play an important role in determining the overall security status of an information system and the ultimate risk to the operations and assets of the organization should that system be placed into operation or continued in its operation.
NIST SP 800-61	Computer Security Incident Handling Guide	1/2004	Security-related threats have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. This document discusses the following topics: (1) organizing a computer security incident response capability; (2) handling incidents from initial preparation through post-incident lessons learned phase; and (3) handling specific types of incidents including denial of service, malicious code, unauthorized access; inappropriate usage, and multiple component incidents.

Tool, Standard, or Publication*	Name	Date	Purpose
NIST SP 800-66	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act Security Rule	3/2005	This publication summarizes the HIPAA security standards and explains some of the structure and organization of the Security Rule. This rule focuses on the safeguarding of electronic protected health information (EPHI). All HIPAA-covered entities, which include some Federal agencies, must comply with the Security Rule, which focuses on protecting the confidentiality, integrity, and availability of EPHI as defined in the rule. The entity that creates, receives, maintains, or transmits EPHI must protect against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. NIST standards and guidelines can be used to support the requirements of HIPAA.
NIST SP 800-83	Guide to Malware Incident Prevention and Handling (Draft)	4/2005	This document provides recommendations for improving an organization's malware incident prevention measures through several layers of controls. It also gives extensive recommendations for enhancing an organization's existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones. The guide focuses on providing practical strategies for detection, containment, eradication, and recovery from malware incidents in managed and non-managed environments.
NIST SP 800-100	Information Security Handbook: A Guide for Managers	10/2006	This Information Security Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program. Typically, the organization looks to the program for overall responsibility to ensure the selection and implementation of appropriate security controls and to demonstrate the effectiveness of satisfying their stated security requirements.

* These documents have been developed by NIST in furtherance of its statutory responsibilities under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996. For further information, see http://csrc.nist.gov/publications/nistpubs/indexhtml.

Table A4-27: Some Representative Tools, Standards, or Publications for Assessing Automated Systems (Listed Alphabetically)

Tool or Standard	Sponsor or Owner	Purpose
BS7799 (Also known as the ISO17799 standard)[76]	BS7799 Security Management Group	BS7799 is one of the most widely recognized security standards in the world, evolving by 2000 into BS EN ISO 17799. It is comprehensive in its coverage of security issues, containing a significant number of control requirements. Compliance using this standard can be achieved across 10 topics: security policy; organization; asset classifications; personnel; physical security; communications; access control; development; continuity; and compliance.
Control Objectives for Information and Related Technology (COBIT)[77]	Brigham Young University	COBIT identifies 34 IT processes, a high-level approach to control over these process, 318 detailed control objectives, and audit guidelines to assess the processes. COBIT provides a broadly applicable and accepted standard for good IT security practices to support management's needs in determining and monitoring the appropriate security and control.
Cyber Input-Output Inoperability Model (CIIM)[78]	University of Virginia	The University of Virginia's Institute for Information Infrastructure Protection (I3P) is developing the CIIM, which will analyze the behavioral, organizational, and psychological factors affecting risk reduction for a networked information system.
Generally Accepted Information Security Principles (GAISP)[79]	Information Systems Security Association	GAISP collects information security principles that have proven themselves in practice and are accepted by most IT security practitioners. It documents those principles in a single repository titled Generally Accepted Information Security Principles (Version 3.X).
Information Security Forum (ISF)[80]	Information Security Forum	The ISF provides a free publication entitled The Standard of Good Practice for Information Security (January 2005). This publication is intended to help any organization, irrespective of market sector, size, or structure, keep the business risks associated with its information within acceptable limits. It is a major tool in improving the quality and efficiency of security controls applied by an organization.
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)[81]	Carnegie Mellon Software Engineering Institute	OCTAVE is a risk-based strategic assessment and planning technique for computer security. It is driven by operational risk and security practices. Technology is examined only in terms of security practices. The OCTAVE criteria define a standard approach for a risk-driven, asset-based, and practice-based information security evaluation. There are two recognized methods that meet OCTAVE criteria. These include the OCTAVE method for large organizations, and OCTAVE-S for smaller organizations. Other methods are under development by third parties.
Qualitative Methodology for the Assessment of Cyberspace-Related Risks	RAND	This 1996 paper discusses the assessment of risk without resorting to quantitative methods that can appear to offer more accuracy and precision than warranted. The authors propose a methodology with three strengths: (1) it is transparent; (2) it does not pretend greater accuracy than can be justified; and (3) it is believed to capture key elements and interactions involved in assessing cyberspace risk.

[76] www.iso17799-made-easy.com.

[77] https://audit.byu.edu/website/tools/COBIT.

[78] www.sys.virginia.edu/risk/projects.html.

[79] www.gaisp.org.

[80] www.isfsecuritystandard.com/home.htm.

[81] www.cert.org/octave.

Tool or Standard	Sponsor or Owner	Purpose
Systems Security Engineering Capability Maturity Model (SSE-CMM)[82]	Systems Security Engineering Working Groups	SSE-CMM is a process reference model. It is focused on the requirements for implementing security in a system or series of related systems that constitute the information technology security domain. The model is intended to be used as a tool for engineering organizations to evaluate security engineering practices and define improvements to them, as a standard mechanism for customers to evaluate a provider's security engineering capability, and as a security engineering evaluation organization.

Table A4-28: Selected ISO Standards Related to IT Security

ISO Standard	Name	Purpose
ISO 13335[83]	Management of Information and Communications Technology Security	This standard has five parts: (1) concepts and models for information and communications technology security management; (2) information security risk management; (3) techniques for the management of IT security; (4) selection of safeguards; and (5) management guidance on network security.
ISO 13569[84]	Information Security Guidelines for Financial Services	This standard provides guidelines for the development of a security program for institutions in the financial services industry, including a discussion of the policies, organization, and the structural, legal, and technical components of such a program.
ISO 15408[85]	Common Criteria for Information Technology Security Evaluation	This is a multi-part standard to be used as a basis for evaluation of security properties of IT products and systems. It essentially enables comparability assessments between different products.
ISO 17799[86]	A Code of Practice for Information Security Practice	This standard for overall information security practices is organized in 10 major sections: (1) business continuity planning, (2) system access control, (3) system development and maintenance, (4) physical and environmental security, (5) compliance, (6) personnel security, (7) security organization, (8) computer and network management, (9) asset classification and control, and (10) security policy.
ISO/PRF TS 21091[87]	Health Informatics: Directory Services for Security, Communication, Identification of Professionals and Patients	This standard is currently under development.

Note: The International Organization for Standardization (ISO) is a network of national standards institutes of 156 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is a nongovernmental organization. For additional information, see www.iso.org.

82 www.sse-cmm.org/model/model.asp.

83 www.iso.org/iso/en.

84 www.iso.org/iso/en/CatalogueDetailPage.

85 www.iso15408.net.

86 www.iso.org/iso/en/CatalogueDetailPage.

87 www.iso.org/iso/en/CatalogueDetailPage.

Appendix 5: Summary of Sector Protective Programs

5.1 DHS Offices, Programs, and Systems Applicable to the Sector

In accordance with HSPD-7, DHS has overall responsibility for leading, integrating, and coordinating the national effort to assess and enhance CI/KR protection efforts.[88] HHS has been working closely over the past year with DHS, VA, and DoD to ensure timely integration of DHS programs with sector initiatives. DHS offices, programs, and systems that are most relevant to CI/KR protection issues facing the Healthcare and Public Health Sector are described below.

5.1.1 DHS Offices

The **DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)** conducts integrated threat analysis for all sectors. As called for in Section 201 of the Homeland Security Act, HITRAC brings together intelligence and infrastructure specialists to ensure a complete understanding of the risks to U.S. CI/KR. 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. The primary focus of HITRAC is terrorist-related threats.

The **DHS National Infrastructure Coordinating Center (NICC)** is the primary center providing private sector partners a medium for reporting suspicious activity that could signal pre-operational terrorist activity.

5.1.2 DHS Programs

The **Protected Critical Infrastructure Information Program**[89] was established pursuant to the Critical Infrastructure Information Act of 2002. This program provides a means for sharing private sector information with the government while providing assurances that the information will be exempt from public disclosure and will be properly safeguarded. This enables members of the private sector to voluntarily submit sensitive information to DHS with the assurance that the information will be protected. The final PCII rule was published September 1, 2006.

Under the **CI/KR Protection-Related R&D Program**, DHS collaborates with SSAs to sponsor CI/KR protection-related R&D, demonstration projects, and pilot programs that enable the advancement of technologies to mitigate protection gaps.

DHS Grant Programs were established under the Homeland Security Act of 2002 for promoting homeland security topics, including the Law Enforcement Terrorism Prevention Program, the State Homeland Security Program, the Targeted Infrastructure Protection Program, and the Urban Areas Security Initiative.[90]

88 National Infrastructure Protection Plan, July 2006, p. 18.

89 National Infrastructure Protection Plan, July 2006, Section 4.3, Protection of Sensitive CI/KR Information, p. 67.

90 These programs are summarized in the National Infrastructure Protection Plan, Section 7: Providing Resources for the CI/KR Protection Program, January 2006, pp. 110-111.

The **Buffer Zone Protection Program (BZPP)** was designed to reduce vulnerabilities of CI/KR sites by extending the protected area around a site into the surrounding community and supporting the prevention and preparedness efforts of local first-responders. BZPP grants provide funding for equipment and for management of these protective actions.

5.1.3 DHS Systems

The Homeland Security Information Network (HSIN) provides a means for sharing DHS information (except data requiring special protections) electronically through the HSIN portal.[91] This information-sharing network consists of components that are connected by a national Web-based communications platform, allowing security partners to obtain, analyze, and share information. HSIN provides two-way and multi-directional information sharing between DHS; the Federal intelligence community; Federal departments and agencies; State, local, and tribal jurisdictions; and the private sector. The connectivity of the network also allows these partners to share information and coordinate among themselves (e.g., State-to-State coordination).

The National Asset Database (NADB), when complete, is expected to contain a listing of all major assets in the United States within all sectors identified in HSPD-7. During 2006, HHS contributed information on 490 major healthcare and public health assets to the NADB to assist in this effort.

5.2 HHS Offices, Programs, and Systems

Significant HHS offices, programs, and systems are described below.

5.2.1 HHS Offices

The **HHS Office of Preparedness and Emergency Operations (OPEO)** coordinates HHS responses to bioterrorism, public health and medical threats and emergencies, and CI/KR protection issues. OPEO has the following responsibilities:

- Develops security-related policies and procedures to manage the Department's responsibilities with regard to sector-specific risks, threats, and vulnerabilities;
- Leads HHS response activities under the National Response Plan;[92]
- Manages the Secretary's Operations Center;
- Trains and directs the Secretary's Emergency Response Teams, including the U.S. Public Health Service (PHS) Tier-1 Rapid Deployment Force teams, the Tier-2 Applied Public Health and Mental Health Teams, and Tier-3 PHS Commissioned Officers available for response to natural disasters and terrorist attacks;[93]
- Coordinates and executes the HHS Continuity of Operations and Continuity of Government programs; and
- Plans, implements, and evaluates departmental and interagency response exercises.

The HHS Departmental Security Council facilitates the coordination of security operations department-wide. Each of the 12 subordinate operating/staff divisions of HHS is represented on the Departmental Security Council by a lead security officer. The Departmental Security Council is responsible for the development of policy recommendations and the formulation of strategic plans. Its members are expected to both participate in council activities and serve as security liaisons for the organizations they represent. The efforts of the council are largely focused on infrastructure protection initiatives.

91 *National Infrastructure Protection Plan*, Section 4.2.3, Information-Sharing Approach, July 2006, p. 60.

92 See DHS, *National Response Plan* (as updated), November 2004.

93 These teams are a recent HHS initiative resulting from recommendations of the White House Task Force; they assess the national response to Hurricane Katrina.

5.2.2 HHS Programs

The HHS risk management framework provides for the identification and coordination of security assurance requirements across all divisions. This framework has evolved over time based on changing missions, enterprise architecture requirements, and the emergent threat environment. Successful implementation of this framework ensures that CI/KR are identified, vulnerabilities are addressed, and risks are mitigated. Specific activities under HHS' risk management program are detailed below.

The **Certification and Accreditation (C&A) Program**, in accordance with FISMA requirements, ensures the confidentiality, integrity, and availability of agency information and the information systems that maintain that data. C&A is accomplished by assessing system vulnerabilities, establishing thresholds for risk acceptance, and identifying and implementing mitigation strategies. Security accreditation provides a form of quality control and ensures that the most effective security controls possible are implemented in an information system.

The **Physical Security Program** provides the appropriate policies, procedures, and technologies to ensure that a high-level security posture is maintained throughout organizational offices, laboratories, storage areas, utilities, and support systems. HHS physical infrastructure facilitates risk mitigation and establishes suitable operating conditions for all staff and information systems.

Personnel Security defines the appropriate policies and procedures to assess an individual's (i.e., contractors, vendors, visitors, and all personnel) suitability to access HHS resources and information.

Continuity of Operations Planning focuses on providing procedures, capabilities, and resources to sustain an organization's essential strategic functions at an alternate operating site for up to 30 days. Integral to this process, HHS has identified specific Priority Mission Essential Functions that support National Essential Functions and which would require restoration following an adverse event. Such functions include emergency medical and public health services; biosurveillance, protection of the food and water supply, and drug supply protections; emergency public health communications; and safe and adequate blood products.

Incident Response, Secure One Communications Center (SOCC), centralizes the HHS cyber incident reporting capability. The SOCC ensures collaboration among all HHS divisions, the Office of the Inspector General, and US-CERT.

HHS Protection Initiatives include administering programs and providing funding to support individual States in the development of biosurveillance systems. Funding is intended to improve infectious disease surveillance and to develop the surge capacity needed to deal with large-scale incidents. The funds allow recipient healthcare organizations to expand laboratory capabilities; invest in interoperable, extensible communications systems; and develop mechanisms for real-time disaster response capabilities.

Project BioShield accelerates research, development, availability, and purchase of effective medical countermeasures against chemical, biological, radiological, and nuclear (CBRN) agents. Through contracts with private industry, Project BioShield has made significant progress in the acquisition of an armamentarium of medical countermeasures to protect the Nation against CBRN threats. Companies with Project BioShield acquisition contracts are required to have established security plans for the development, manufacturing, storage, and distribution of work performed under contract. ASPR security experts provide technical advice to these companies on security matters in accordance with the principles of industrial security, thus safeguarding U.S. Government contracts from corporate security program deficiencies.

Under the **Project BioShield Contractor/Security Director Communications Program**, HHS Office of Security Programs personnel conduct regular teleconferences with U.S. Government contractor security directors. Security program infractions are discussed in detail, and security directors are provided with assistance in developing corrective actions. This format for regular, ongoing dialog has proven to be effective in forming mature interagency working relationships and enhancing current corporate security programs, including infrastructure protection.

Under the Bioterrorism Hospital Preparedness Program, the Health Resources and Services Administration (HRSA) distributes funding to State health divisions to help ensure that hospitals are prepared for potential chemical, bioterrorism, and radiological attacks, and other threats. As a condition of receiving HRSA funding, the program requires that facilities conduct vulnerability assessments aimed at helping them better focus their grant applications.

HRSA/DHS CI/KR Protection-Related Site Visits have been made to approximately 10 private sector hospitals per year over the past 2 years in connection with the Bioterrorism Hospital Preparedness Program. During these visits, conducted in connection with Federal grant programs requiring grant recipients to meet security standards, joint HHS/DHS teams perform a wide range of CI/KR protection-related assessments.

Under **CDC Cooperative Agreements**, CDC provides grants and other assistance to State and local agencies on a wide range of public health issues, including chemical, biological, and radiological attacks.[94] Many of these cooperative agreements have CI/KR protection-related components or implications. Site visits in connection with these cooperative agreements could potentially incorporate CI/KR protection assessments and encourage the development of protective programs.

Under the **International Early Warning Surveillance Program**, HHS helps protect the health of Americans, in cooperation with the Secretariat of the World Health Organization and other technical partners, by leading U.S. Government efforts in surveillance and detection of disease outbreaks overseas.

Border States Initiatives are programs through which HHS continues to build the capacity of the public health systems of all 20 U.S. border States (including Alaska) to provide cross-border early warning of infectious diseases. These initiatives seek to enhance the infectious disease surveillance capabilities and prompt sharing of findings among U.S. States and tribal nations, Mexican states, Canadian provinces, and Canadian First Nations along the border.

BioWatch detects the release of pathogens into the air, warning the government and public health community in the event of a potential bioterror event. The entire list of pathogens, for which BioWatch tests, is not publicly available.

The **Biosurveillance Initiative** enhances the Nation's ability to prevent the introduction and spread of disease caused by a bioterrorism agent originating abroad, and to detect domestic outbreaks early. This initiative increases the number of quarantine stations at major ports of entry and extends BioSense, CDC's near-real-time human health surveillance system, to additional users in States and metropolitan areas.

5.2.3 HHS Systems

CI/KR Protection-Related Information Systems sponsored by ASPR include three information systems that track specific infrastructure-related data that can be used in emergencies. The first is a system to track burn bed capacity across the United States, helping ensure that the Nation's capacity for treating burn patients will be utilized properly in emergencies. The second is a pilot critical infrastructure data system to track the status of major healthcare and public health facilities during emergencies such as hurricanes. The third is a system sponsored by the Agency for Healthcare Research and Quality that aggregates information from disparate information systems that track hospital status information.

More generally, HHS is a major sponsor and/or significant participant in systems used to capture, analyze, and disseminate information related to bio-threats of all kinds. These systems play a variety of information-sharing roles across the Healthcare and Public Health Sector as a whole. Principal systems sponsored by HHS or its major security partners are summarized in table 8-1.

[94] See Sarah A. Lister, Specialist in Public Health and Epidemiology, Domestic Social Policy Division, An Overview of the U.S. Public Health System in the Context of Emergency Preparedness, Congressional Research Service, Library of Congress, March 17, 2005, CRS-8.

5.3 Department of Veterans Affairs CI/KR Protection Program

Health programs under the Veterans Health Administration (VHA) include approximately 163 hospitals and an additional 1,100 points of care within the United States, Guam, Puerto Rico, and the Philippines. VA healthcare sites are inspected by the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) on an independently established schedule. Among other factors, JCAHO accreditation criteria include critical infrastructure protection measures.

5.3.1 VA Offices

The **Office of Cyber and Information Security**, which manages the Critical Infrastructure Protection Program, as well as the IT Information Security Program, has overarching responsibility for assessing, mitigating, and defending against cyber security threats, including those facing the veterans health system. This program is intended to not only protect the VA infrastructure, but also to respond to and mitigate the effects of crisis events that would otherwise impede business-critical functions. Tasks related to the CI/KR protection mission include monitoring internal and external threat capabilities, implementing protective measures, responding to active threats and attacks, continuously monitoring system and external boundary security measures, providing continuity of operations in the event of a disaster, and fulfilling support roles under ESF-8 of the National Response Plan.

The **Office of Cyber and Information Security Review and Inspection Division**, in conjunction with the Office of Facilities Management and the Office of Security and Law Enforcement, has responsibility for conducting yearly assessments of the physical security of VA facilities. These assessments are intended to uncover vulnerabilities that would allow access into the facilities and leased structures housing VA staff and information systems.

5.3.2 VA Programs

The **Healthcare Facility Inspection Program** assures that VA healthcare facilities meet all applicable requirements. As it would not be cost-effective to assess all VA facilities yearly, only a percentage of facilities are inspected. The criteria for inspection are based on the size of the facility, scope of services, number of servers, certification and accreditation results, and other IT-related surveys.

5.3.3 VA Systems

VHA has established a survey assessment tool focused on medical center emergency preparedness. This tool helps analyze facility and staff preparedness in areas such as medical center backup utilities, laboratory and pharmacy facilities, psychiatric services, security, administration, and internal medicine. The Web-based survey assessment tool provides for follow-up assessments at regular intervals. VHA has also established an analytical Physical Security Database to track progress in addressing identified infrastructure vulnerabilities.

5.4 DoD CI/KR Protection Program

DoD has developed a defense-wide, fully integrated, and sustainable program for protecting CI/KR vital to national and economic security.[95] The DoD CI/KR protection framework is designed to meet these objectives as CI/KR protection requirements change, and to carry out support roles under ESF-8 of the National Response Plan.[96]

[95] Additional information on the DoD CI/KR protection program can be found in the DoD Critical Infrastructure Protection Plan for Healthcare, Spring 2006.

[96] As of September 2006, The National Response Plan contained 15 Emergency Support Function (ESF) Annexes: (1) Transportation, (2) Communications, (3) Public Works and Engineering, (4) Firefighting, (5) Emergency Management, (6) Mass Care, Housing, and Human Services, (7) Resource Support, (8) Public Health and Medical Services, (9) Urban Search and Rescue, (10) Oil and Hazardous Materials Response, (11) Agriculture and Natural Resources, (12) Energy, (13) Public Safety and Security, (14) Long-Term Community Recovery and Mitigation, and (15) External Affairs. Each ESF description contains a description of roles, responsibilities, participants, and related topics.

5.4.1 DoD Offices

DoD Health Affairs has the overall responsibility for the DoD healthcare system worldwide. On CI/KR protection issues, DoD Health Affairs has four objectives: (1) identifying critical assets, conducting vulnerability assessments, and taking mitigating actions to provide mission assurance; (2) determining intra-dependencies within the health sector capability areas and interdependencies with all defense sections; (3) interfacing with databases containing real- or near-real-time data; and (4) coordinating with Federal, State, and local governments to integrate or supplement DoD-held data with data from other initiatives.

The **Armed Forces Medical Intelligence Center (AFMIC)** acts as the focal point within DoD for compiling all-source intelligence and producing finished intelligence on foreign military and civilian medical capabilities. Subjects include the health status of foreign military forces, infectious disease and environmental health risks, and scientific and technical developments in biotechnology and biomedical subjects of military importance.

5.4.2 DoD Programs

DoD CI/KR protection capability areas consist of the following: (1) critical medical materiel, (2) medical materiel supply chain, (3) blood, (4) medical research, (5) preventive medicine and public health, (6) healthcare information networks, (7) emergency medical operations centers, (8) patient evacuation, (9) deployable medical units, and (10) medical treatment facilities.

5.4.3 DoD Systems

DoD Health Affairs uses a critical infrastructure tool called Primary Health Assets Staging Tool (PHAST).[97] This unclassified, Web-based application with over 12,000 assets provides near-real-time visibility into medical assets and capabilities for informed decision-making. Comprehensive asset information includes both critical and non-critical assets. PHAST has Geographic Information System capabilities tied to other sectors. It contains real-time and updated information that can be searched in the areas of capability/capacity, geographical, functional, and proximity data.[98]

5.4.4 Department of Labor

Within the DOL, OSHA aims to ensure worker safety and health by working with employers and employees to create better working environments. Since 1971, OSHA has helped to cut workplace fatalities by more than 60 percent and occupational injury and illness rates by 40 percent. At the same time, U.S. employment has doubled from 58 million workers at 3.5 million worksites to more than 115 million workers at 7.2 million sites.

OSHA seeks to assist the majority of employers while focusing its enforcement resources on sites in more hazardous industries—especially those with high injury and illness rates. Less than 1 percent of inspections—about 300—fell under OSHA's Enhanced Enforcement Program. Strong enforcement has helped to increase alleged violations by more than 10 percent over the past 5 years, including an increase of 14 percent in alleged willful violations since 2003. At the same time, injuries and illnesses continue to decline significantly.

5.5 Private Sector Programs

Numerous private sector security programs are conducted in response to specific industry, competitive, or local concerns. Most of these are conducted as a part of an integrated risk management program. Among other activities, such programs allow

[97] Ten capability areas are cataloged by PHST: (1) medical treatment facilities, (2) blood support, (3) medical materiel supply chain, (4) critical medical materiel items, (5) deployable medical units, (6) medical research, (7) healthcare information systems, (8) emergency medical operation centers, (9) patient evacuation, and (10) preventive medicine/public health. Each capability has been assigned a lead within DoD who is responsible for ensuring that areas are updated. A total of 29 systems and 12,000 assets have been documented. Description supplied by OASD (HA) during September 2006.

[98] Description supplied by OASD (HA) during September 2006.

insurance companies to determine exposure, risk, and appropriate premium rates. Many are not publicized for proprietary, competitive, or security reasons. Some examples are cited below.

5.5.1 Accreditation Reviews

Nearly all healthcare and public health organizations must be periodically accredited by an industry-approved external body. The accreditation process involves meeting accepted standards across a broad range of topics. Physical security, workforce protection, and cyber security play varying roles in such accreditation reviews.

The **Joint Commission on the Accreditation of Healthcare Organizations (JCAHO)** plays an important role in promoting effective protective programs across a broad front. JCAHO currently accredits approximately 15,000 healthcare facilities, including 4,300 hospitals on a 3-year cycle. Laboratories are accredited every 2 years. One major aspect of the accreditation process is unannounced site visits by JCAHO assessment teams. Since 2001, these assessments have examined each facility's disaster plan, including its relationships with all important stakeholders in its community. Since failure to achieve accreditation can result in a facility's inability to receive Medicare/Medicaid funds, JCAHO assessments are taken seriously by the facilities.

Related Accreditation Bodies include the National Committee for Quality Assurance, which evaluates managed care plans for patient safety, confidentiality, consumer protection, and continuous improvement.[99] Another example is the Continuing Care Accreditation Commission, acquired by the Commission on Accreditation of Rehabilitation Facilities in 2003, which accredits a broad range of long-term care facilities.[100] A third is the Council on Accreditation, an international, independent, non-profit accrediting body for over 60 types of social assistance programs.[101-102]

5.5.2 Pharmaceutical Industry

While not mandated by legislation to conduct risk assessments or modify its security practices relative to CI/KR protection requirements, the multi-national pharmaceutical industry has many incentives to reduce threats to its facilities, systems, and workforce personnel. Increases in drug counterfeiting, drug re-importation, and drug diversion, for example, have escalated the need for strong pharmaceutical security measures among manufacturers, distributors, retailers, and regulatory agencies.[103] In addition, the pharmaceutical industry must protect itself against industrial espionage, terrorism, and natural disasters. Given the importance of these protective programs to the industry, it is believed that they are effectively self-policed.

5.5.3 Public/Private CI/KR Protection Programs

InfraGard is an information-sharing and analysis effort serving the CI/KR protection interests and combining the knowledge base of a wide range of members. Not exclusively devoted to healthcare and public health, InfraGard is an association of businesses, academic institutions, State and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. Each InfraGard section works closely with program managers at FBI headquarters.[104]

The goal of InfraGard is to promote ongoing dialogue and timely communication among members. InfraGard members gain access to information that enables them to protect their assets. In turn, members provide information that helps the government fulfill its responsibilities to prevent and address terrorism and other crimes.

99 See www.ncqa.org/communications for further information.

100 See www.carf.org/aging for more information.

101 See www.coa.org.

102 State licensing boards may also be a source of information concerning key facilities and functions.

103 Navigant Consulting, Inc., April 1, 2003, Publication ID: CDCQ1144784.

104 Details on InfraGard can be found at www.infragard.net.

Appendix 6: Coordinating Council Member Organizations

GCC Member Organizations

The Department of Health and Human Services, including the following Operating Divisions:

- The Centers for Disease Control and Prevention
- The Food and Drug Administration
- The Healthcare Resources and Services Administration
- The National Institutes of Health
- The Administration for Healthcare Research and Quality

The Department of Homeland Security

The Department of Defense

The Department of Veterans Affairs

The Department of Agriculture

The Association of State and Territorial Health Officials

The National Association of County and City Health Officials

The National Indian Health Board

The Association of Public Health Laboratories

SCC Member Organizations

American Association of Blood Banks

American Association of Occupational Health Nurses, Inc.

American Hospital Association

American Industrial Hygiene Association

American Medical Association

American Nurses Association

America's Health Insurance Plans

BIO - the Biotechnology Industry Organization

Blue Cross & Blue Shield Association

DST Output

Evidence Based Research, Inc.

Health Information and Management Systems Society

Henry Schein, Inc.

International Cemetery and Funeral Association

Joint Commission on Accreditation of Healthcare Organizations

LabCorp

National Funeral Directors Association

Nevada Hospital Association

Pharmaceutical Research and Manufacturers of America

The Regional Medical Center

University of Pittsburgh Medical Center

Homeland Security

Department of
Health and
Human Services