Healthcare and Public Health Sector-Specific Plan

May 2016

Homeland Security

Coordination Letter from Council Chairs

In 2003, the Federal Government established the Healthcare and Public Health (HPH) Sector as a critical infrastructure sector in the United States, recognizing that its security and resilience are essential to national security, the economy, and public health and safety. Since that time, the Sector has built strong partnerships that bring together private sector owners, operators, and professional associations with government representatives at the Federal, State, and local levels. Together, these partners have improved information sharing, developed guidance and tools, and conducted training and exercises to improve incident response and recovery. The HPH Sector recognizes the value of this partnership and continues to coordinate to improve security and resilience.

2016 Sector-Specific Plan Update

The release of the 2016 HPH SSP reflects the maturation of the HPH Sector partnership and the progress of the sector programs first outlined in the 2007 and 2010 Sector-Specific Plans (SSPs). Changes from previous SSPs include a streamlined and updated set of goals and objectives and an increased emphasis on priorities such as information sharing and emergency response. The 2016 SSP represents a continued collaborative effort among the private sector; Federal, State, local, tribal, and territorial governments; and nongovernmental organizations to develop specific membership actions over the coming years required to reduce critical infrastructure risk and enhance Sector resilience.

The HPH Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) jointly developed the goals, priorities, and activities included in this SSP to reflect the overall strategic direction for the HPH Sector. The Sector's goals support the Joint National Priorities developed in 2014 by the national council structures described in the National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (NIPP 2013).

This SSP also illustrates the continued maturation of the HPH Sector partnership and the progress made to address the Sector's evolving risk, operating, and policy environments.

The HPH Sector continues to take steps to better understand all-hazards risks and implement appropriate actions to mitigate corresponding impacts at all levels of government and the private sector throughout the Nation's Critical Infrastructure.

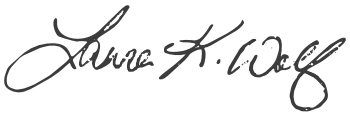
Key Accomplishments

Since 2010, the HPH Sector partners in the public and private sectors have taken significant steps to reduce sector risk, improve coordination, and strengthen security and resilience capabilities:

- Both the SCC and GCC undertook extensive outreach programs. State, local, and private sector partners were recruited through presentations, webinars, and outreach to national associations.
- The Homeland Security Information Network portal for the HPH Sector was expanded to better meet the information sharing needs of the Sector including a lessons learned repository and the addition of over 1300 documents to enhance relevant situational awareness for end-users.
- A full methodology is under development for use in assessing the risks to the Sector including cyber, physical, and human vulnerabilities and threats.

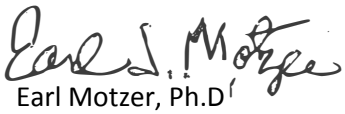
- Sector partners collaborated to develop a comprehensive Active Shooter Training Guide and Suspicious Activity Reporting Guide for Sector facility end-users. Both documents have been utilized extensively in the public and private sector.
- The SCC and GCC collaborated to establish a Joint Cyber Working Group to enhance cyber security engagement throughout the Sector.

The SCC and GCC are pleased to support this SSP and look forward to sustaining and enhancing the security and resilience of critical infrastructure in the HPH Sector.



Laura K. Wolf, Ph.D

Primary Chair, HPH Sector
Government Coordinating Council
U.S. Department of Health and Human Services



Earl Motzer, Ph.D

Primary Chair, HPH Sector
Coordinating Council

Don R. Boyce, JD

Deputy Assistant Secretary
Director, Office of Emergency Management
U.S. Department of Health and Human Services

Caitlin Durkovich

Assistant Secretary
Office of Infrastructure Protection
U.S. Department of Homeland Security

Table of Contents

1 Executive Summary

This Healthcare and Public Health (HPH) Sector-Specific Plan (SSP) is designed to guide the Sector's internal and collaborative, cross-sector efforts to enhance the security and resilience of HPH critical infrastructure to all-hazards across its physical, cyber, and human dimensions. The SSP tailors the strategic guidance provided in the *National Infrastructure Protection Plan* 2013 (NIPP 2013) to the unique operating conditions and risk landscape of the vast and complex HPH Sector.

The Sector's integrated approach to managing all-hazards risks to HPH critical infrastructure and the HPH workforce includes several key components:

- Identifying and preparing for a range of potential threats and hazards;
- Reducing the vulnerabilities of identified critical assets, systems, and networks, including those associated with critical internal and out-of-sector dependencies and interdependencies;
- Mitigating the potential impacts to and enabling the timely restoration of critical infrastructure as a result of emergencies that do occur; and
- Adapting to changing conditions to withstand and rapidly recover from disruptions due to emergencies, irrespective of the causal factors.

Effective implementation of this approach is guided by two core tenets: collaborative risk management and public-private sector partnership.

Vision, Mission, and Goals

The strategic direction for efforts to enhance and sustain the security and resilience of HPH Sector critical infrastructure is informed by the vision detailed in the NIPP 2013, as well as by the "Call to Action" and the Joint National Priorities established by the NIPP partnership structure. The HPH Sector vision, mission, and goals are identified below. They were derived through consideration of a number of important factors, including national and sector policy and risk management priorities, resource availability, risk reduction progress made to date, known capability gaps, and emerging risks. Over the next four years, these goals will help drive collective action across the Sector, tailored to reflect considerations of HPH subsector, regional, and local public and private partners.

Sector Partnership Vision

A public-private partnership supporting the needs of HPH Sector critical infrastructure and Federal, State, local, tribal, and territorial (FSLTT) government partners to enhance resilience of the Sector to all hazards.

Sector Partnership Mission

To sustain the essential functions of the Nation's healthcare and public health delivery system and to support effective emergency preparedness and response to nationally significant hazards. Public and private sector partners will evaluate risks; coordinate plans and policy; and provide guidance to prevent, protect, mitigate, respond to, and recover from all hazards that pose a threat to the Sector's critical infrastructure.

Sector Partnership Goals

- Risk Assessment: Leverage relationships and resources to assess and analyze threats to, vulnerabilities of, and consequences of disruption to HPH Sector critical infrastructure to inform risk management activities. Ensure that approaches consider the physical, cyber, and human elements of critical infrastructure security and resilience, supply chain issues, and interdependencies with other sectors.
- Risk Management: Enhance the resilience of the HPH Sector by translating risk analyses into actionable recommendations for State and local public health departments, individual private sector facilities, and health systems at large. Integrate such risk analyses into the mitigation, response, and recovery efforts of the Federal Government. Execute risk mitigation activities in a prioritized manner with clear plans and metrics for success.
- Information Sharing: Enhance existing and develop new mechanisms to ensure bidirectional sharing of information. Promote sharing of risk information, threats, best practices, and lessons learned between government and private sector partners.
- Partnership Development and Coordination: Develop and implement a "Partnership Engagement Strategy" to include outreach efforts to both government and private sector entities with a focus on developing relationships with owners and operators of critical infrastructure. Encourage development of regional; State, local, tribal, and territorial (SLTT); cross-sector; and intra-HPH Sector partnerships to enhance sector resilience, facilitate information sharing, and respond to disasters.
- Response and Recovery: Engage in response and recovery efforts across FSLTT government agencies, health care coalitions, and the private sector during and after disasters, including cybersecurity incidents. Exercise the ability of the Sector to respond to natural or manmade disasters and incorporate lessons learned into future exercises and corrective actions.

Measuring Effectiveness

The U.S. Department of Health and Human Services (HHS), in coordination with other HPH Sector partners, has the primary responsibility for the management and measurement of sector-wide progress toward achieving the goals and priorities identified in this SSP using a combination of relevant metrics. The metrics contained in this SSP represent a starting point from which to capture appropriate quantitative and qualitative feedback related to achievement of the Sector's key near-term priorities.

2 Introduction

Managing all-hazards risks to critical infrastructure in the HPH Sector requires a comprehensive and integrated approach to:

Identify Risks

- Identify and prepare for a range of potential threats and hazards.

Reduce Vulnerabilities

- Reduce the vulnerabilities of identified critical assets, systems, and networks, including those associated with critical internal and out-of-sector dependencies and interdependencies.

Mitigate Impacts

- Mitigate the potential impacts to critical infrastructure and enable the timely restoration of functionality when events and incidents do occur.

Enhance Resilience

- Adapt to changing conditions to withstand and rapidly recover from disruption due to emergencies, irrespective of the cause of the disruption (manmade or natural).

The success of such an approach depends on the ability to leverage a broad spectrum of authorities, capabilities, expertise, experience, and resources from an array of public and private sector stakeholders. Additionally, efficient sharing of actionable and relevant information among partners is required to build situational awareness and enable effective risk-informed decision-making during both steady-state and emergency response operations.

The purpose of this SSP is to guide and integrate the Sector's efforts to secure and strengthen the resilience of HPH critical infrastructure across its physical, cyber, and human dimensions. In addition, this SSP describes how the HPH Sector contributes to the national critical infrastructure mission area priorities, as set forth in Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience,*[1] and Executive Order (E.O.) 13636, *Improving Critical Infrastructure Cybersecurity*,[2] and the National Preparedness Goal (NPG) as set forth in PPD-8, *National Preparedness*

[1] The White House, Presidential Policy Directive 21, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[2] The White House, Executive Order 13636, Improving Critical Infrastructure Security and Resilience, https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

This SSP is also aligned with the *National Health Security Strategy* (NHSS) *and Implementation Plan 2015-2018*,[3] the goal of which is to provide strategic direction to ensure that efforts to improve health security nationwide are guided by a common vision, based on sound evidence, and carried out in an efficient, collaborative manner.

This SSP reflects the strategic guidance provided in the NIPP 2013,[4] and is tailored to the unique operating conditions and risk landscape of the HPH Sector. As such, it establishes a sector-level vision, mission, goals, and supporting activities, all of which are guided by two core tenets: collaborative risk management and public-private sector partnership. Together, these SSP components help inform security and resilience planning and preparedness investments within the HPH Sector. Figure 1 illustrates the overarching components of the SSP Framework and how the two core tenets, collaborative risk management and public-private sector partnership, influence vision, mission, goals, and supporting activities. These efforts in turn lead to effective critical infrastructure planning and preparedness.

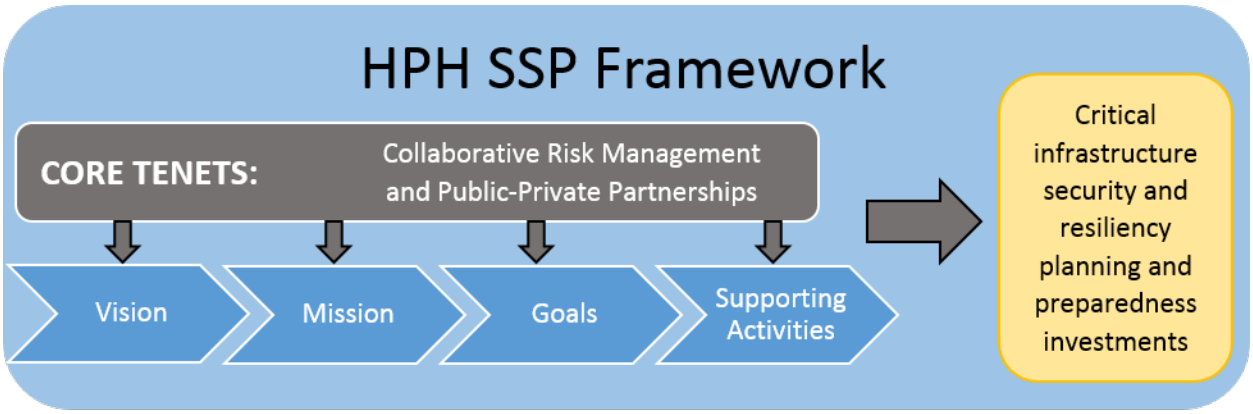


Figure 1. HPH SSP Framework

This SSP represents a collaborative effort among the private sector; SLTT governments; and Federal departments and agencies to achieve the overarching goal of reducing critical infrastructure risk. The Plan also reflects the maturation of the HPH Sector partnership, and builds upon the progress made by the Sector since the issuance of the 2010 SSP to address the evolving critical infrastructure risk, operational, and policy environments. The updates to the 2010 SSP provided in this plan also are informed by experience gained and lessons learned from real world incidents, exercises, and training activities that have occurred over the past six years.

This 2016 HPH SSP builds upon previous SSP iterations by emphasizing the complementary goals of security and resilience for critical infrastructure. Major changes from the 2010 version include*:*

- An updated Sector profile, including identification of the principal threats and hazards the Sector faces;

[3] Department of Health and Human Service, National Health Security Strategy, http://www.phe.gov/Preparedness/planning/authority/nhss/Documents/nhss-ip.pdf
[4] Department of Homeland Security, National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience, http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

- Discussion of the Sector's principal information sharing mechanisms, including those related to cybersecurity and incident response;
- Updated Sector vision and mission statements, partnership goals, and near-term priorities and implementation activities;
- Identification of linkages to key policy directives and the NIPP 2013 Call to Action and Joint National Priorities;
- Important updates to the NIPP 2013 Risk Management Framework, tailored to the unique operating and risk environments of the HPH Sector;
- Mapping of the Sector's critical infrastructure security and resilience activities to preparedness and incident management priorities under PPD-8 and the National Preparedness System; and
- Identification of performance metrics mapped against near-term priorities to provide ongoing feedback regarding progress toward achieving Sector goals.

The audience for this SSP includes a wide-ranging critical infrastructure community comprised of Federal departments and agencies, SLTT government organizations, international partners, private sector owners and operators, and other private and non-profit organizations with important roles to play in securing and strengthening the resilience of HPH Sector critical infrastructure. This SSP is also intended to serve as an important repository of information for other sectors under the NIPP 2013 partnership framework, as the essential functions and workforce populations of those sectors are critically dependent on the HPH Sector. Finally, this SSP, as a publicly accessible document, also can help inform the general public and Congress on efforts to achieve critical infrastructure security and resilience within the HPH Sector.

3 Sector Overview

3.1 Introduction

The HPH Sector provides goods and services integral to maintaining local, national, and global health security. HPH Sector resources are critical in supporting the five core mission areas (prevention, protection, mitigation, response, and recovery) as discussed in PPD-8 and the NHSS, as well as in safeguarding Sector assets, people, and the communities they serve before, during, and after any incident with actual or potential health consequences.

HPH Sector infrastructure is largely dedicated to building and sustaining community health resilience; enhancing and expanding the Nation's medical capacity for everyday healthcare; improving health-related situational awareness capabilities; enhancing the integration of HPH capabilities into emergency management systems in effective ways; and strengthening global health security. Key elements of the HPH Sector are integrated and scalable from baseline operations to crisis response mode anywhere in the U.S.

The domestic response to Hurricane Katrina in 2005, the H1N1 influenza pandemic in 2009, Superstorm Sandy in 2012, and the Ebola epidemic in West Africa in 2014 demonstrated how important the HPH Sector can be during a national challenge or health crisis.

Disruption of the HPH Sector also can directly impact the American economy. HHS estimates that 17.4 percent ($2.9 trillion) of our Nation's 2013 gross domestic product was spent on healthcare.[5]

3.2 Sector Profile

The HPH Sector is large, diverse, and open, spanning both the public and private sectors. It includes publicly accessible healthcare facilities, research centers, suppliers, manufacturers, and other physical assets and vast, complex public-private information technology systems required for care delivery and to support the rapid, secure transmission and storage of large amounts of HPH data.

Access to healthcare is critical in maintaining national health security. In 2011, Americans made 262 million visits to hospital emergency or outpatient departments. At any one time, almost 50 percent of Americans require one or more prescription medications to mitigate health issues.[6] For many Americans, even a brief disruption in HPH services could be catastrophic.

National demand for HPH infrastructure is extremely high. In 2012, America's 15,673 certified nursing homes operated at over 80 percent capacity, and, at any one time, over 60 percent of the beds in America's 4,973 community healthcare facilities were occupied.[7] With such high demand, even minor interruptions to local or regional HPH infrastructure can have widespread impacts.

Reforms, like the Patient Protection and Affordable Care Act, stimulate innovation in patient care and healthcare delivery, which not only provide great benefits to patient health, but also may inadvertently introduce potential vulnerabilities, particularly from an information security perspective. Similarly, the broad implementation of health information technology (Health IT) and the growing reliance of health situational awareness upon cost-effective real-time data transmission enhance the efficiency and cost-effectiveness of health care; however, communication failures or cyber disruptions of these technologies can present serious consequences.

The HPH Sector's critical infrastructure can be classified according to service types and functional categories, or subsectors, resulting in six private and two government subsectors. The functional composition of the various subsectors will be reviewed periodically to ensure their continued relevance and inclusivity. Private and government HPH subsectors are briefly described in Figures 2 and 3, respectively.

[5] National Center for Health Statistics. "Health, United States, 2013: With Special Feature on Prescription Drugs." United States Department of Health and Human Services. Hyattsville, MD 2014. http://www.cdc.gov/nchs/data/hus/hus13.pdf
[6] Ibid.
[7] Ibid.

HPH Private Subsectors

Direct Patient Care

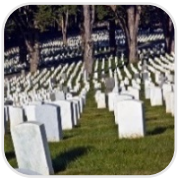
This is the largest subsector, encompassing healthcare systems, professional associations, and a wide variety of medical facilities, public health, and emergency medical services. It employs over 12 million Americans. According to the American Hospital Association, this subsector supports 5,686 registered healthcare facilities with more than 900,000 staffed beds.[8] Over 35 million citizens are admitted to these facilities annually.

Health Information Technology

This subsector includes medical research institutions, information standards bodies, and electronic medical record systems vendors. With the adoption of the Patient Protection and Affordable Care Act and incentives of up to $2 million, statistics from HealthIT.gov indicate that 59 percent of America's hospitals,[9] 95 percent of America's community pharmacies, and 40 percent of America's office-based physicians[10] have adopted electronic health records.

Health Plans and Payers

Health insurance companies and plans, local and State health departments, and State emergency health organizations in this subsector employ over 500,000 Americans. Outside of private insurers, the Centers for Medicare and Medicaid Services report that the Medicare, Medicaid, and Children's Health Insurance programs cover more than 100 million Americans.



Mass Fatality Management Services

Approximately 133,000 Americans work in cemetery, cremation, morgue, and funeral home occupations. This subsector also includes mass fatality support services such as coroners, medical examiners, forensic examiners, and psychological support personnel. The subsector remains dominated by small employers; approximately 86 percent of funeral homes are owned by families, individuals, or closely held companies with, on average, 3-5 full-time employees.

Medical Materials

The medical supply chain depends upon the 600,000 Americans who work in the public and private sectors in the areas of medical equipment and supply manufacturing and distribution. The Healthcare Distribution Management Association reports that pharmaceutical distributors alone deliver 15 million prescription medicines and healthcare products to more than 200,000 licensed healthcare providers in all 50 states.

Laboratories, Blood, and Pharmaceuticals

A mix of government and private sector assets, this subsector is critical for healthcare situational awareness, and includes pharmaceutical manufacturers, drug store chains, pharmacists' associations, public and private laboratory associations, and blood banks. According to HealthIT.gov, 95 percent of the pharmacies in the Nation are actively e-prescribing, and over 32 percent of new prescriptions are sent electronically.[11]

Figure 2: HPH Private Subsectors

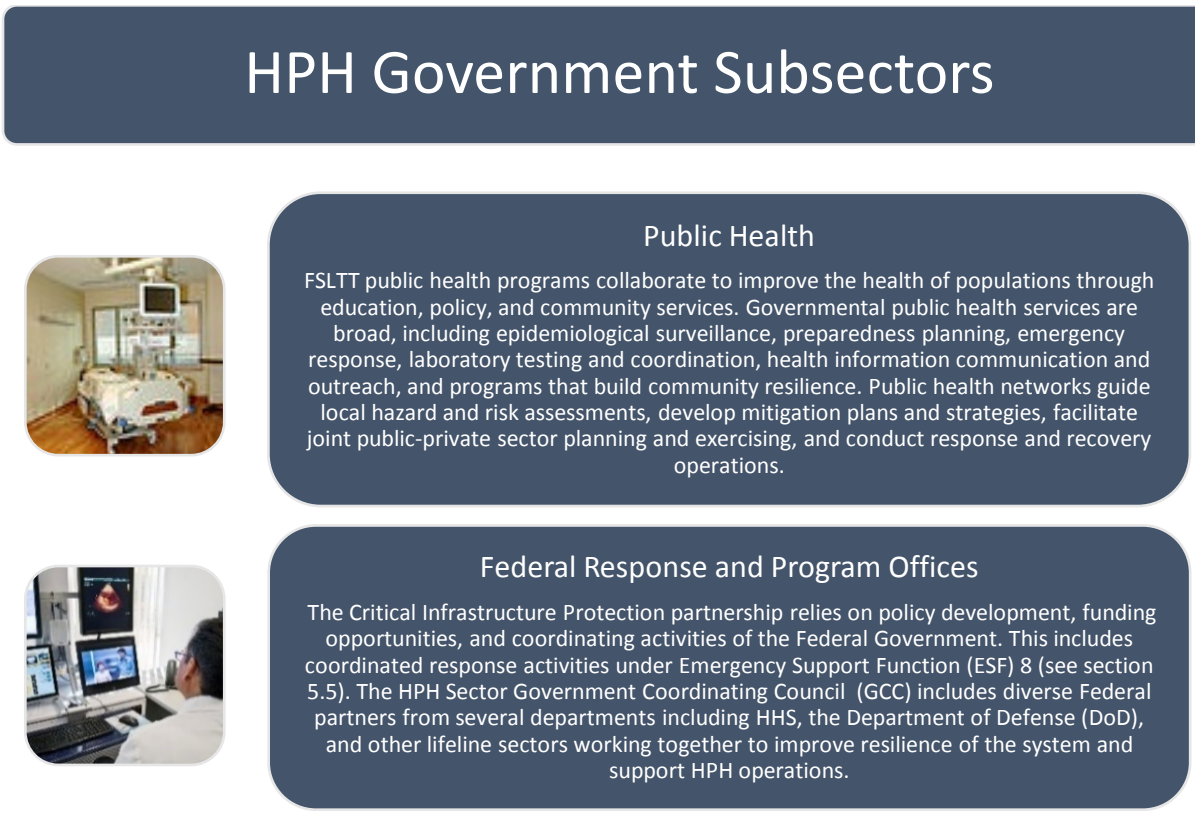


Figure 3: HPH Government Subsectors

Over 14 million workers, representing more than 10 percent of the total American workforce, are employed in the HPH Sector throughout the U.S. This includes those who provide services directly to healthcare recipients and those who play a supporting role, such as vaccine manufacturers.[11] Figure 4 illustrates the vast distribution of employees across the HPH community nationwide (both public and private) that provide direct, population-based care, emergency response, and other public health and disease surveillance functions (e.g. doctors, dental hygienists, therapists, etc.). Given this landscape, HPH Sector infrastructure security and resilience are ultimately defined by the ability of the Sector to prevent or mitigate negative impacts upon the delivery of HPH services.

[8] Health IT, ONC Data Brief, No 16: Adoption of Electronic Health Record Systems among U.S. Non-federal Acute Care Hospitals: 2008-2013, May 2014, https://www.healthit.gov/sites/default/files/oncdatabrief16.pdf

[9] Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, Update on the Adoption of Health Information Technology and Related Efforts to Facilitate the Electronic Use and Exchange of Health Information: A Report to Congress (June 2013), https://www.healthit.gov/sites/default/files/rtc_adoption_of_healthit_and_relatedefforts.pdf

[10] Ibid.

[11] Bureau of Labor Statistics. United States Department of Labor. "Current Employment Statistics." http://www.bls.gov/web/empsit/ceseeb1a.htm

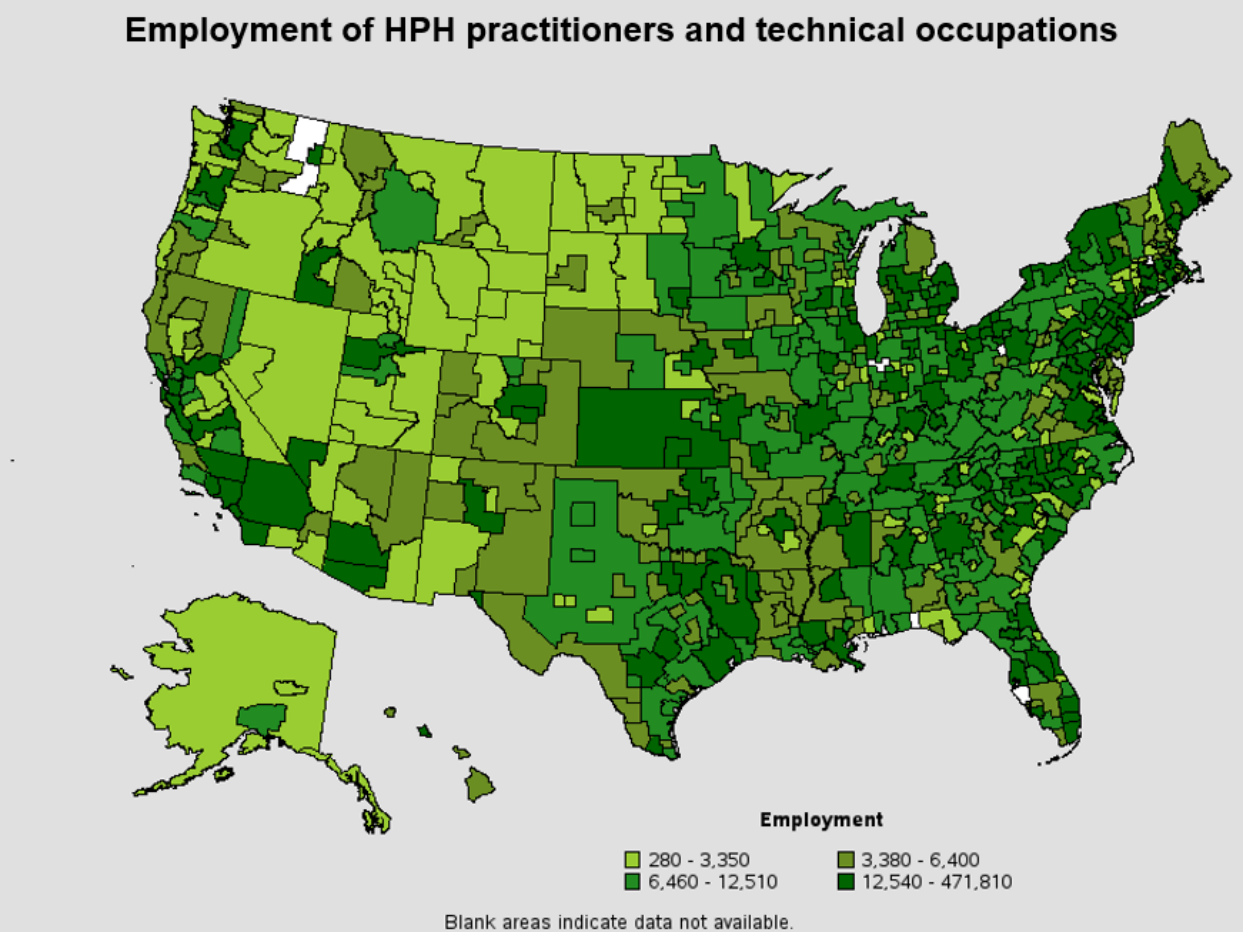


Figure 4: Employment of HPH practitioners and technical occupations (public and private), by area (May 2014. This map shows that the density of HPH Sector employees is roughly comparable to density of population in the United States. [12]

3.3 Sector Risks

The size, diversity, openness, and economic value of the HPH Sector make it an attractive potential target for terrorists or other malicious actors. In the event of a natural disaster or other event, increased demand for HPH services, coupled with potentially degraded interdependent infrastructures, may impact the ability of the Sector to adequately meet surge demands during an incident with health consequences.

The NHSS notes that these risks can be "exacerbated by vulnerabilities that vary from community to community." These variations represent differences in fiscal health, numbers of at-risk individuals, levels of training and exercising for health security, and the availability of countermeasures for emerging

[12] Bureau of Labor Statistics. United States Department of Labor. "Occupational Employment and Wages, May 2014." http://www.bls.gov/oes/2014/may/oes290000.htm

infectious diseases. These factors complicate risk assessment and response, making active community engagement a vital part of overall HPH Sector security and resilience.

3.4 Emerging Sector Threats and Hazards

Pandemics and Health Crises: Emerging and re-emerging diseases can put HPH Sector personnel at risk and severely impact HPH operations. The U.S. is constantly at risk regarding the emergence of new diseases, such as Severe Acute Respiratory Syndrome (SARS) and Middle East Respiratory Syndrome (MERS), or the onset of a severe influenza pandemic. At the same time, long-standing problems, like increasing antibiotic resistance and supply shortages, stress health care systems. For example, multidrug resistant bacteria represent a direct challenge to healthcare facilities, posing a hazard to patients, HPH workers, suppliers of diagnostic equipment, and health facilities themselves. The White House National Action Plan for Combating Antibiotic-Resistant Bacteria, released in March 2015, estimates that at least two million illnesses and 23,000 deaths are caused by drug-resistant bacteria in the U.S. each year.[13]

Natural Disasters, Extreme Weather, and Climate Change: The HPH Sector is represented at every level of community across the Nation, making the entire Sector (facilities, employees, information systems, supply chains, etc.) vulnerable to natural disasters. Ongoing climate change will lead to more extreme weather events in the years to come and exacerbate other scenarios, as described in Figure 7. Figures 5 and 6 provide examples of impacts to the HPH Sector during and following the Joplin Tornado (2011) [14] and Superstorm Sandy (2012).[15] The challenge of mitigating operational disruptions while meeting increased demand is a persistent concern as conveyed in these examples.

On May 22, 2011, an EF5 Tornado ripped through the town of Joplin, Missouri, killing 161 people

- **Critical HPH infrastructure was destroyed**: St. John's Regional Medical Center was destroyed, forcing the evacuation of 177 patients. Six patients were killed during the tornado.
- **Vulnerable populations were disproportionately impacted:** Three of the city's six skilled nursing facilities were hit before residents could be moved to safer areas. At least 11 died, and almost 200 residents were displaced.
- **Such a severe event stresses the health of the public:** The Centers for Disease Control (CDC) reported that an uncommon, and potentially fatal, fungal infection had been found in over a dozen people who had been injured in the storm. The CDC explained that due to the stresses of such an event, human immune systems may be weakened for a time.

Figure 5: Effects of the Joplin, MO, tornado

[13] The White House, National Action Plan for Combating Antibiotic-Resistant Bacteria, March 2015, https://www.whitehouse.gov/sites/default/files/docs/national_action_plan_for_combating_antibotic-resistant_bacteria.pdf

[14] The White House. Joplin: One Year Later, https://www.whitehouse.gov/joplin; Centers for Disease Control and Prevention, Tornado Survivors Battle Deadly Fungus in Joplin, Missouri (August 1, 2011), http://blogs.cdc.gov/publichealthmatters/2011/08/tornado/

[15] Adalja, Watson, Bouri, Minton, Morhard, and Toner. Absorbing Citywide Patient Surge During Hurricane Sandy: A Case Study in Accommodating Multiple Hospital Evacuations. *Annals of Emergency Medicine* (2014); Treperman. Hurricane Sandy and the greater New York health care system. *Journal of Trauma and Acute Care Surgery* (2013).

Superstorm Sandy hit the New York metropolitan area on October 29, 2012, impacting local, regional, and national health security

- **Infrastructure Failure**: Lack of water and power forced most hospitals to close after the storm made landfall. Only a single hospital remained open in Manhattan.
- **Patient Evacuations:** At least 37 health care facilities (acute, nursing, long-term care, etc.) were evacuated after the storm hit, displacing more than 6,300 residents and hindering first-responders from supporting other priorities.
- **Delayed Treatment:** More than 40 percent of the region's dialysis centers were closed. Six hundred dialysis patients were displaced in the Chinatown-lower Manhattan area alone, raising the risk of patient morbidity and mortality.
- **Long-Term Care Disruption:** Approximately 90 percent of the roughly 100 opiate treatment programs in New York City shut down, eliminating support when stress and other factors contributing to addict relapse were highest.

Figure 6: Effects of Superstorm Sandy

Malicious Human Acts: Dissemination of a biological or chemical agent; use of a radiological, nuclear, or explosive device; or an attack on a critical HPH Sector facility by malicious actors, domestic extremist groups, or international terrorist organizations could cause mass casualties; attract undue media attention; and lead to local, regional, or national disruption of the delivery of vital services. The disruptive potential of violent "lone actors" or malicious insider attacks on mission-critical infrastructure is a growing concern both inside and outside the Sector. Active shooter incidents remain a persistent threat to healthcare facilities, even as overall gun-homicide rates have decreased over the last decade.

Supply Chain Disruption and Corruption: Incredibly efficient supply chains have resulted in a "just-in-time" delivery model that may leave the HPH Sector with very limited inventories, diagnostic capabilities, or capacity in an emergency, making many healthcare providers sensitive to cascading consequences in the context of a system-level disruption or corruption. Approximately 92 percent of HPH Sector stakeholders are private sector entities.[16] Therefore, if key supplies are unable to reach private sector healthcare providers and facilities, or if reach-back support is eliminated, patients will be directly impacted by disruptions and delays in HPH operations. In addition, rapid global transportation networks can unintentionally disseminate diseases, adulterated pharmaceutical supplies, tainted blood products, or contaminated food widely with unprecedented speed.

Cyber Attacks: The HPH Sector is increasingly dependent upon health IT and the secure storage and transmission of individually identifiable health information to dictate care, maintain patient records, control financial operations, etc. A recent report reveals that nearly half of pharmaceutical and life science organizations experienced a breach of security within a 12-month time span.[17] Malicious cyber actors may aim to harvest personal data, corrupt information, or impact financial security. Additionally,

[16] Government Accountability Office, Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics, p.28, http://www.gao.gov/assets/260/252603.pdf

[17] Greif, Eschbach, De Jong, Muller, Annino, Timm, Koch, Mathis, Berthaut, and Metcalf (2014). Defending Yesterday: Key Findings from the Global State of Information Security Survey 2014. *Pricewaterhouse Coopers.*

larger-scale disasters or attacks on the electronic backbone or supporting infrastructure can disrupt data access across the entire HPH Sector, which, in turn, could impact patient care directly.

Malware exploits, sophisticated viruses, and Advanced Persistent Threats have been identified as significant security threats to the pharmaceutical industry and the HPH Sector at large. Additionally, intellectual property theft through cyberattacks can threaten competitiveness, innovation, and research and development (R&D), particularly in areas where proprietary research provides a competitive advantage.

Space Weather and Electromagnetic Pulse (EMP) Risks: Technology on the earth is vulnerable to potentially severe space weather. In particular, the Nation's power grid is at risk of being damaged or rendered ineffective by the effects of an EMP—a sudden burst of electromagnetic radiation (pulse) resulting from a natural or manmade event. Naturally occurring EMPs are produced as part of the normal cyclical activity of the magnetic storms that flare from the surface of the sun. Depending on the impact area, an EMP event could be catastrophic for healthcare facilities, causing long-term power outages that may overwhelm the Sector's backup power sources.

Building Healthcare Sector Resilience

Ongoing climate change will lead to more extreme weather events and exacerbate other scenarios. This will put a progressively greater strain on the HPH Sector as public health emergencies become more common. To help healthcare facilities better prepare for the future, HHS published a report of best practices entitled *Primary Protection: Enhancing Health Care Resilience for a Changing Climate*. HHS has also developed a climate change resilience toolkit. Additional information on Building Health Care Sector Resilience is available at http://toolkit.climate.gov/topics/human-health/building-climate-resilience-health-sector.

Figure 7: Resources for Preparing for Climate Change

Internal HPH Sector Dependencies and Interdependencies: The size and complexity of the HPH Sector tie the concept of Sector resilience to a number of important intra-sector dependencies, interdependencies, and related challenges. Due to the increasingly interconnected nature of the Sector's physical and cyber components, even a single point of failure within the HPH Sector can cause cascading impacts throughout. For example, the 2009 H1N1 pandemic highlighted the importance of the medical supply chain in providing the drugs, vaccines, medical devices, and personal protective equipment needed for workforce protection.[18]

Cross-Sector Dependency and Interdependency Risks: The HPH Sector is closely integrated with other sectors, which creates dependencies and interdependencies that can cause disruptions in one sector to very quickly and profoundly impact operations in another. Local disasters can cascade to multiple jurisdictions and interdependent sectors, triggering disruption across larger geographic areas. Limited awareness of the risks related to sector dependencies and interdependencies may subject an

[18] Bush, Haydn (2011). Reliance on Overseas Manufacturers Worries Supply Chain Experts. *Hospital and Health Networks Journal.*

organization to “hidden risks”—meaning those risks that it assumes another entity can adequately manage.

Cross-Sector Dependency and Interdependency Risks (cont.): The HPH Sector could not function without resources and services provided by many other sectors, in particular, the so-called “lifeline functions”—transportation, communications, energy, and water—as well as emergency services. These sectors provide necessary goods and services that support nearly every home and business across the country, are commonplace in everyday life, and are critical to disaster response and community resilience. These sectors involve complex physical assets and electronic networks and interconnections with other critical sectors. A disruption in one or more of these sectors has the potential to cause cascading effects to multiple other sectors. Addressing potential loss of lifeline functions supports preparedness planning and capability development vital to Sector security and resilience. Figure 8 describes the HPH Sector dependencies on the lifeline sectors and the Emergency Services Sector (ESS).

Through Sector partnerships and cross-sector collaboration, the HPH Sector must factor critical dependency and interdependency issues into contingency plans and, to the extent possible, consider alternative means of communication, transportation, and provision of water and energy to sustain operations during an emergency that affects the lifeline sectors and the ESS.

HPH Sector Lifeline Function Dependencies

Energy

All healthcare facilities require energy to operate; thus facilities' varying abilities to remain self-sustaining during a significant power failure emergency threaten the Sector as a whole. Further, energy is needed to support the operations of other interdependent sectors, such as providing power to the Water and Communications Sectors for necessary services.

To mitigate this reliance, the HPH Sector should utilize generators to the extent possible in a disaster scenario. Additionally, energy requirements, including emergency fuel needs, should be assessed in order to prioritize limited energy availability in the event of an outage.

Transportation Systems

The HPH Sector relies on transportation for the efficient shipment of supplies, without which the Sector cannot provide healthcare services. Transportation of raw materials, pharmaceuticals, personnel, emergency response units, patients, and fatalities is critical to vital HPH functions. During a disaster, emergency personnel and equipmnt must reach those in need of care, or be able to transport the injured to a healthcare facility.

Water and Wastewater Systems

Water is a basic human need and is vital to human health. The HPH Sector relies on potable water and wastewater for infection control, sanitation, renal dialysis, laboratory needs, heating and air conditioning, manufactoring and storage of pharmaceuticals, sterilization, maintenance of blood and organ banks, drinking water for staff, and a myriad of other uses.

To mitigate this reliance, the HPH Sector should identify the services that must remain operational to provide healthcare to patients, determine the quantity of water necessary for continuity during a water service interruption, plan for potential impacts of water loss on all aspects of healthcare, determine alternative water sources and incorporate them into response plans, and coordinate with other sectors to facilitate the sharing of resources if necessary.

Communications

The HPH Sector requires communications infrastructure to maintain situational awareness and coordinate healthcare activities during steady state and emergency response. Radio and telephone communications can support a wide variety of business processes. During an emergency, communications are essential to provide information to the public as well as to facilitate the sharing of resources throughout the sector.

To mitigate this reliance, plans should be put in place in advance of a disaster to direct the actions of healthcare providers in the absense of communications resources or before communications can be restored.

Emergency Services

The ESS consists of emergency services facilities and associated systems, as well as trained and tested personnel to provide life safety and security via the first-responder community. Its mission is closely intertwined with the HPH Sector mission of supporting emergency response preparedness and operations. The HPH Sector relies heavily on ESS as the Nation's first line of defense and prevention, and for its role in the short-term mitigation of consequences immediately following a disaster. Speed and coordination with ESS in the aftermath of an incident are critical to HPH life-saving activities.

Figure 8: HPH Sector lifeline function and emergency services dependencies

3.5 Inherent Sector Vulnerabilities

With a community focus and ethos of open service, the HPH Sector is inherently more vulnerable than many of the other critical infrastructure sectors. Many key HPH facilities are publicly accessible by design, with little or no ability to physically limit entry or screen those seeking access. The diversity of the Sector also complicates efforts to assess and mitigate risk. Key HPH infrastructure varies from community to community; hence, no single template or operational procedure for security or resilience is uniformly applicable across the entire HPH Sector.

The HPH Sector is large and highly distributed, reaching into every community. The HPH Sector also is overwhelmingly dependent on highly trained, credentialed specialists that safeguard America's healthcare system. Loss of key personnel, especially at the local level and in rural communities where personnel redundancy may be an issue, can be even more disruptive and carry a greater impact than the loss of a key facility.

3.6 Potential Incident Impacts and Consequences

Community-by-community variations in fiscal health, numbers of at-risk individuals, levels of training in health security, and availability of countermeasures for emerging infectious diseases, among other factors, complicate consequence management. As the 2014-15 Ebola epidemic in West Africa demonstrated, the impact and consequences of an isolated, geographically-distant incident can cascade quickly, becoming a widespread—even global—crisis. Also, as demonstrated by the tornado that struck Joplin, Missouri, in 2011, or Superstorm Sandy in 2012 (Figures 5 and 6, respectively), the consequences of an incident can be both physical and psychological in nature, affecting services and audiences far beyond the actual physical impact zone. Similarly, the health-related impacts of a broader incident can be focused on a single municipality or carry with them long-term, cascading impacts on vulnerable populations (e.g., those that are prescription-dependent, immune compromised, pregnant, or require oxygen or dialysis, etc.) distributed across a wide geographic area.

3.7 Critical Infrastructure Partnerships

The best way to advance collective action towards HPH Sector infrastructure security and resilience is through voluntary collaboration among private sector and government stakeholders. The HPH Sector operates under the NIPP partnership structure, which encourages participation from across the Sector, as well as partnerships with other critical sectors. The success of this model depends on the ability to leverage capabilities, expertise, and experience from across the critical infrastructure community and associated stakeholders. Efficient sharing of actionable and relevant information among Sector partners builds situational awareness and enables effective, risk-informed decision-making that may benefit the entire Sector.

Collaboration within the partnership is afforded unique protection through the Critical Infrastructure Partnership Advisory Council (CIPAC). Under CIPAC, the Secretary of Homeland Security can exercise statutory authority to exempt CIPAC meetings from certain requirements of the Federal Advisory

Committee Act. These exemptions facilitate the flow of advice and potentially sensitive information concerning critical infrastructure security and resilience and incident communications. Members comply with restrictions against activities such as lobbying and influence-peddling in order to protect information while maintaining public trust.

3.8 Sector Coordinating Structures

The NIPP partnership framework is built upon the imperative to bring together public and private sector partners to coordinate security and resilience efforts at the sector-level. To accomplish this aim, in accordance with PPD-21, HHS serves as the Sector-Specific Agency (SSA) for the HPH Sector and is responsible for managing and coordinating broad-based sector security and resilience activities. The HHS Secretary has delegated leadership responsibility for PPD-21 implementation and other activities under the NIPP 2013 to the Office of the Assistant Secretary for Preparedness and Response (ASPR).

ASPR serves as the Secretary's principal advisor on public health emergencies and leads a collaborative approach to the department's preparedness, response, and recovery portfolio. ASPR is also the lead office responsible for all Federal public health and medical response to public health emergencies and incidents covered by the National Response Framework (NRF) and National Disaster Recovery Framework. See Appendix D for additional information on ASPR programs relevant to critical infrastructure security and resilience.

ASPR has established the Critical Infrastructure Protection (CIP) Program Office to manage its responsibilities under PPD-21, E.O. 13636, and the NIPP 2013. The CIP Program Office is fully integrated with ASPR's broader mission, which enables the program to leverage ASPR's relationships for improved collaboration with Sector stakeholders to advance infrastructure security and resilience. For additional information on the HHS ASPR CIP Program, including its role in national critical infrastructure policy implementation and in coordinating HPH infrastructure security and resilience with Sector partners, please refer to the PHE website.[19]

Under the NIPP 2013, government and private sector entities share responsibility for securing and enhancing the resilience of HPH Sector critical infrastructure. As the SSA, HHS is responsible for bringing together leaders in business and government to prepare for and protect against all hazards facing the Sector. The HPH Sector partnership identifies and prioritizes the most critical elements of the Nation's HPH infrastructure, shares information on risks impacting that infrastructure, and implements activities to protect and enhance the resilience of the Sector. The partnership consists of a Government Coordinating Council (GCC) made up of government partners and a Sector Coordinating Council (SCC) made up of private sector partners. The two councils collaborate through a number of joint working groups. The SCC/GCC partnership model is illustrated in Figure 9. This model works by organizing individual SCC and GCC working groups and then creating jointing working groups which convene to cover matters of joint concern.

[19] Public Health and Medical Emergency, Critical Infrastructure Protection for the Healthcare and Public Health Sector website at http://www.phe.gov/preparedness/planning/cip/Pages/default.aspx

Both the SCC and GCC aim to expand participation over the course of this SSP term. To do so, the Councils plan to review current membership composition and participation, scan the Sector to identify gaps in expertise, and identify potential new member organizations from within the Sector.

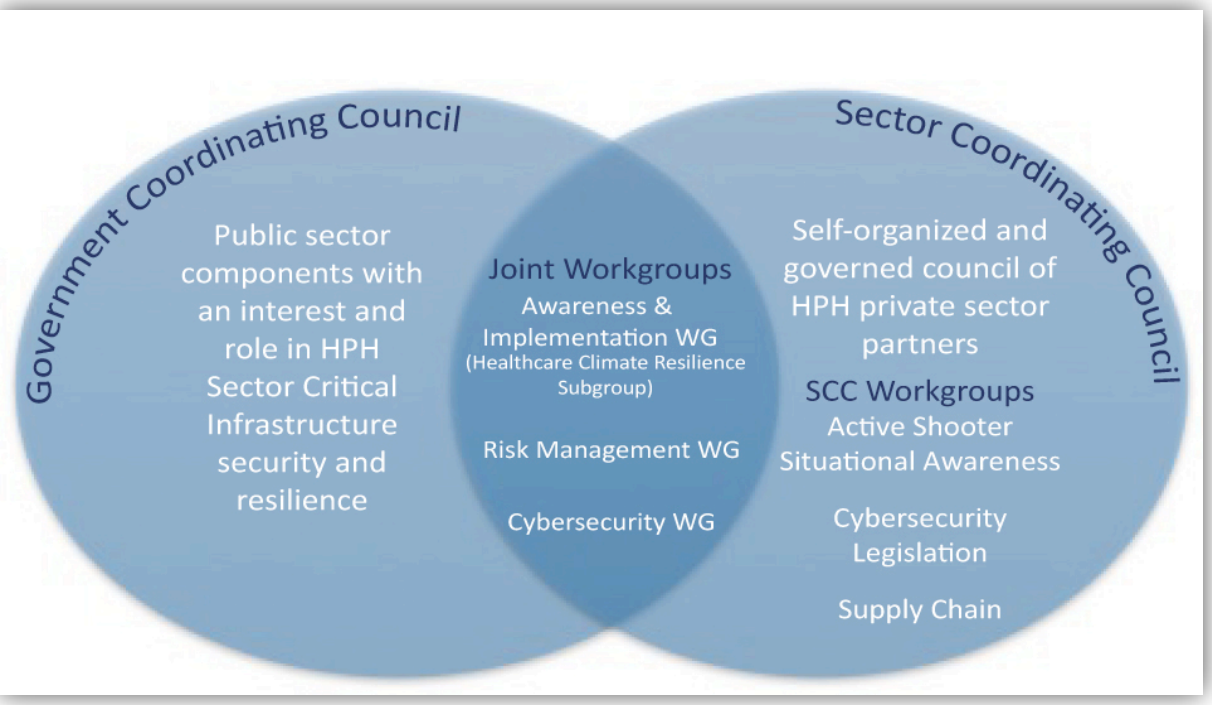


Figure 9: SCC/GCC Partnership Model. The GCC and SCC represent the key organizing elements of the HPH Sector Partnership. Key activities are supported by a number of joint working groups.

3.8.1.1 Sector Coordinating Council

The SCC is a self-governing body made up of representatives of privately owned and operated healthcare facilities, nongovernmental organizations, trade associations, and professional societies that operate within the healthcare arena. The SCC provides a forum for partners to discuss private sector interests and perspectives in the public-private effort to protect and enhance the resilience of HPH critical infrastructure. The SCC mission is two-fold: first, to service the needs of owners and operators in regard to preparing for, responding to, and recovering from all hazards; and second, to represent the interests of the private sector to FSLTT agencies and to inform government policy, plans, and programs relevant to HPH infrastructure security and resilience.

The SCC is organized into six standing subcouncils that represent the major HPH private subsectors, as discussed above in section 3.2. The six private sector SCC subcouncils are: Direct Patient Healthcare; Health Information Technology; Health Plans and Payers; Mass Fatality Management Services; Medical Materials; and Laboratories, Blood, and Pharmaceuticals.

Members of the SCC participate in standing workgroups (WGs) that monitor and manage issues of relevance to the Sector, including active shooter situational awareness, cybersecurity legislation, and supply chain. The WGs undertake long-term projects that produce concrete deliverables to help inform and advise the SCC Executive Committee. Additionally, situationally focused WGs can be formed by the SCC Executive Committee to address specific needs of the subcouncils.

The SCC has established a list of goals to focus its critical infrastructure security and resilience efforts:

- Integrating cyber and physical risk management;
- Improving resilience decision-making and incorporating resilience into each stage of the infrastructure lifecycle with consideration of broader threats (climate change, aging infrastructure, demographic shifts, etc.);
- Strengthening risk management partnerships to enhance national capacity;
- Enhancing incident management to ensure effective and efficient response and recovery;
- Building cost-effective resilient leadership;
- Preparing for active shooter incidents in HPH facilities;
- Developing stronger cross-sector WGs with other sectors; and
- Improving dissemination of classified or other critical information throughout the Sector.

Additional information, including the SCC Charter and membership information, can be found on the Department of Homeland Security (DHS) website.[20]

3.8.1.2 Government Coordinating Council

The HPH GCC is the public sector component of the Sector's public-private partnership framework. The mission of the GCC is to provide effective coordination of HPH Sector risk management strategies and activities, policies, and communication across government agencies and between the government and the private sector. As the HPH SSA, HHS chairs the GCC. The GCC also works to coordinate efforts of FSLTT representatives with regards to the two HPH government subsectors: Public Health and Federal Response and Program Offices. Expertise within the GCC includes SLTT public health departments and professional associations and Federal representatives from departments providing direct patient care, regulatory and policy support, ESF-8 response support, and funding for preparedness and recovery issues.

[20] U.S. Department of Homeland Security, Healthcare and Public Health Sector: Council Charters and Membership website at http://www.dhs.gov/healthcare-and-public-health-sector-council-charters-membership

HHS also works through major State and local HPH professional associations to establish appropriate links with SLTT public health entities. The National Association of County and City Health Officials, the Association of State and Territorial Health Officials, the Association of Public Health Laboratories, and other HPH professional associations have long-standing relationships with both HHS and their respective members. Figure 10 provides an example of the important benefits of close collaboration between all levels of government and local community members and businesses.

Additional information, including the GCC Charter and membership information, can be found on the DHS website.[21]

3.8.1.3 Joint Working Groups

The GCC and SCC come together via joint WGs to address issues of mutual concern. All private and public sector members of the HPH Sector with a role in critical infrastructure security and resilience are invited to take part in the joint WGs. WGs may change depending on the Sector's needs. For example, a new cybersecurity joint WG to address the growing risk of cyberattacks on the HPH sector is a shared, near-term priority of the GCC and SCC. The four GCC/SCC Joint WGs are described in Table 1.

Local Public Health and Community Partnership

Seattle and King County, WA, exemplify the benefits of a strong partnership between local health departments (LHDs) and the communities they serve. King County sought a solution to the resource and personnel intensive task of LHD distribution of medication during a disaster scenario. They turned to existing community resources, particularly the county's 300 local pharmacies, to develop a strategy for emergency medication dispensing. During the 2009 influenza outbreak, the strategy was tested and the public health and pharmacy collaboration proved hugely successful. As a result, interest in the LHD-pharmacy partnership expanded from the county to the state level. In 2012, the Washington State Department of Health developed a Memorandum of Understanding (MOU) and an operational plan to implement the pharmacy agreements statewide. Today, King County continues to expand its LHD-community partnerships, and is currently working with community leaders to increase the existing capacity for mass dispensing of medication, and to meet all health and medical needs of the community during an emergency. Details about the LHD-Pharmacy partnership are available at http://nacchopreparedness.org/?p=3014.

Figure 10: Example of government and community cooperation

[21] U.S. Department of Homeland Security, Healthcare and Public Health Sector: Council Charters and Membership website at http://www.dhs.gov/healthcare-and-public-health-sector-council-charters-membership

Table 1: GCC/SCC Joint WGs. Each WG has specialized expertise and a distinct role to play in enhancing HPH critical infrastructure security and resilience.

Joint Working Group	Role
Risk Management (RMWG)	Acts as lead for sector-level implementation of the NIPP Risk Management Framework; collaborates with stakeholders to identify assets, systems, and networks critical to HPH operations; and develops a list of most critical infrastructure assets within HPH Sector annually.
Awareness and Implementation (A&I WG)	Advises GCC and SCC on critical infrastructure information needs and recommends processes for obtaining and sharing information with Sector partners during steady state and incident response; monitors the Homeland Security Information Network (HSIN)-HPH portal to improve effectiveness and organization and disseminate information; and identifies best practices for improved Sector-wide information sharing.
Healthcare Climate Resilience	Reviews documents as requested as part of the President's Climate Action Plan.
Cybersecurity / Cyber Threats	Addresses emergent cyber-related risks to HPH information and IT systems, including Health IT.

3.8.1.4 Department of Homeland Security

HHS and DHS continually communicate and coordinate on HPH Sector risk management activities. HHS also works with DHS to implement various presidential directives, executive orders, and statutes.

The HPH Sector works in close collaboration with several DHS offices and programs:

DHS Science and Technology (S&T) Directorate: The HPH Sector works closely with DHS S&T to exchange information on R&D needs and priorities for a wide range of research areas.

DHS Federal Emergency Management Agency (FEMA): To fulfill its all-hazards disaster preparedness and response mission requirements, including the review of threat/hazard information and the potential consequences that could result from specific types of all-hazards events, the HPH Sector draws expertise from and collaborates with FEMA on an extensive basis.

DHS Office of Health Affairs (OHA): OHA plays an important role as the principal authority for all medical and health issues for DHS and is the principal advisor on the subject to the Secretary and FEMA Administrator. OHA is an important partner in classified and unclassified information sharing on public health threats and leads an initiative to increase the integration of public health considerations into fusion centers. Many of the Sector's public health threat briefings are co-sponsored by OHA.

DHS National Protection and Programs Directorate (NPPD): NPPD plays a critical role in fostering policies, plans, and programs that serve to strengthen critical infrastructure security and resilience.

Through the *Office of Infrastructure Protection (IP)*, NPPD has established strong relationships with FSLTT agencies and the private sector across all critical infrastructure sectors. Additionally, DHS IP provides overall oversight of the NIPP partnership model, as well as a wide array of key cross-sector outreach and liaison activities. Among these is the Protective Security Advisor Program, the mission of

which is to facilitate infrastructure security and resilience field activities through a distributed liaison presence and to provide access to infrastructure security and resilience resources, training, and information in support of SLTT and private sector partners.

Through the *Office of Cyber and Infrastructure Analysis (OCIA; formerly the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC)),* NPPD maintains a DHS Center of Excellence that analyzes all-hazards consequences to the Nation's critical infrastructure by evaluating the potential disruptions from physical or cyber threats and incidents, including those associated with dependencies, interdependencies, and cascading impacts. OCIA works with the HPH Sector and other partners to produce the congressionally mandated National Critical Infrastructure Prioritization Program Level 1 and Level 2 List and the E.O. 13636 Section 9 List of cyber-dependent critical infrastructure.

Through the *Office of Cybersecurity and Communications (CS&C)*, NPPD works to prevent or minimize disruptions to critical information infrastructure in order to protect the public, the economy, and government services. In addition, the National Cybersecurity and Communications Integration Center (NCCIC) serves as a 24/7 cyber monitoring, incident response, and management center and as a national focal point for cyber and communications incident integration.

Through the *National Infrastructure Coordinating Center (NICC)*, NPPD operates a dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the Federal Government. When an incident or event affecting critical infrastructure occurs and requires coordination between DHS and the owners and operators of our Nation's infrastructure, the NICC serves as that information sharing hub to support the security and resilience of these vital assets.

DHS Office of Intelligence and Analysis (I&A): I&A supports the HPH Sector by providing it with intelligence and information regarding all-hazards threats to Sector critical infrastructure. The HPH Sector can use this information to inform risk-related decision-making and support the security enhancement of key Sector infrastructure.

3.9 Information Sharing and Protection

The HPH Sector invests significant resources to continually expand its information sharing capabilities. The Sector maintains an active A&I WG responsible for overseeing sector information sharing initiatives and activities. These include the ongoing enhancement of the Homeland Security Information Network (HSIN)-HPH portal and its embedded notification and alert capability, maintenance of the public-facing Partnership website, the ASPR-Technical Resources, Assistance Center, and Information Exchange (TRACIE) portal, and annual Joint Sector teleconferences and in-person meetings. In response to all-hazards events, the SSA initiates conference calls and webinars open to the entire Sector to accelerate communications. These information-sharing initiatives deliver considerable value to Sector members and have significantly increased engagement in Sector infrastructure security and resilience activities. Figure 11 provides a detailed example of a unique sector-wide information sharing capability.

The HSIN-HPH portal plays a major role in the SSA strategy to facilitate timely and effective sharing of information among Sector stakeholders. The main site features general content regarding HPH Sector activities, while subsites are dedicated to ongoing incidents (such as the 2014 Ebola response) and the public-private working groups that the Sector maintains. The SSA routinely monitors health-related critical infrastructure information sources and posts relevant content to the portal. This information covers a broad variety of topics, including policy updates, operations, threat and vulnerability information, and cybersecurity issues. For information that is not at the *For Official Use Only (FOUO)* level, the SSA maintains a public website,[22] which includes unclassified information available to the general public.

ASPR activated the TRACIE in 2015.[23] TRACIE features resource materials, a help line, just-in-time suggestions, and tools to share information gleaned from real-life experiences in preparing for, responding to, and recovering from disasters. ASPR developed TRACIE in collaboration with a network of experts nationwide, including SCC and GCC members, to address needs identified by stakeholders charged with preparing for HPH system emergencies. Users can get advice, including just-in-time advice, from hundreds of health care, disaster medicine, public health, and public safety professionals through ASPR TRACIE.

As a mechanism for sharing information on topics of interest to Sector partners, the SSA hosts annual joint meetings of the SCC and GCC. These meetings, held by teleconference and in-person, allow members to meet and share information in both formal and informal settings and help to enhance trust in the partnership. Classified threat briefings are offered to those with appropriate clearances.

Private sector partners enhance cybersecurity information-sharing efforts through Information Sharing and Analysis Organizations (ISAOs). E.O. 13691, *Promoting Private Sector Cybersecurity Information Sharing*, released in 2015, promotes the development of ISAOs through standards-setting activities and encouraging SSAs to address cyber threats by sharing information broadly. Two examples of ISAOs include the National HPH Information Sharing and Analysis Center (NH-ISAC) and the Health Information Trust Alliance (HITRUST).

The NH-ISAC, a private sector, non-profit organization, is the officially recognized ISAC for the HPH Sector by HHS, DHS, the HPH SCC, and the National Council of ISACs (NCI). The NH-ISAC provides a trusted community for the sharing of timely, relevant, and actionable physical and cyber information among stakeholders to help maintain the continuity of the Sector in the context of both cyber and physical risks. As a trusted third party, NH-ISAC facilitates collaboration among members, the HPH Sector, other critical infrastructure sectors, and government partners. Offerings include situational awareness, incident response collaboration, coordination, and the sharing of a wide range of information, such as indicators of compromise, tactics, threat actor techniques and procedures, best practices, and mitigation strategies.

The NH-ISAC has grown rapidly in recent years. Members include direct patient care providers; health information technology companies; health plan payers; medical device manufacturers; and laboratory, blood, and pharmaceutical organizations. As a member of the NCI, the NH-ISAC participates in a number

[22] Public Health Emergency, Critical Infrastructure Protection for the Healthcare and Public Health Sectors website at http://phe.gov/cip

[23] U.S. Department of Health and Human Services, TRACIE website at https://asprtracie.hhs.gov/

of important activities including daily inter-ISAC cyber and weekly physical calls, a secure portal and list-serve used for sharing information, an automated threat indicator sharing mechanism, and training and exercises.

The NH-ISAC also aligns with its peer ISACs and government partners through its presence on the DHS NCCIC and NICC watch floors. At the NCCIC, the NH-ISAC has embedded representatives, cleared at the Top Secret/Sensitive Compartmented Information level, who attend daily briefs and other NCCIC meetings to share information on threats, vulnerabilities, incidents, and potential or known impacts to the HPH Sector. Its presence on the NCCIC and NICC floors enhances situational awareness and information sharing and facilitates collaboration between the HPH Sector, government, law enforcement, and the other critical infrastructure sectors. In addition, representatives from the NH-ISAC participate as members of the Cyber Unified Coordination Group (Cyber UCG), a public/private group that convenes during cyber threats and incidents of national significance and in the Cross-Sector Cyber Security Working Group (CSCSWG), a public/private body that facilitates cross-sector collaboration on cyber issues. NH-ISAC also has a close relationship with the Healthcare SCC and participates on the SCC Executive Committee, as well as with the multiple FSLTT agencies serving the HPH Sector.

Specifically, the NH-ISAC assists the Sector through:

- Delivering timely, relevant, and actionable cyber and physical email alerts from various sources distributed through the NH-ISAC Security Operations Center;
- Facilitating member sharing of threat, vulnerability, incident information, and best practices in a trusted manner using the Traffic Light Protocol to guide information dissemination;
- Facilitating instantaneous member, cross-sector, and government partner sharing of threat intelligence through an automated platform;
- Holding regular threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities, and incidents affecting the critical sectors;
- Hosting two annual conferences where members and Sector stakeholders can network and learn about the latest threats and mitigation strategies;
- Providing rapid response briefings to members when a broad-scale threat or attack is imminent or underway;
- Collaborating with government partners, the HPH Sector, other critical infrastructure sectors, and law enforcement for incident response coordination;
- Surveying members and compiling results for situational awareness and best practice sharing;
- Delivering emergency threat or incident notifications to all members using Ready Op, an emergency notification system;
- Participating in various cyber exercises such as those conducted by DHS (i.e., the Cyber Storm and Capstone Exercise series) and cross-sector exercises such as the Operational Collaboration Forum Series conducted by the NCI; and

- Engaging with other critical infrastructure sectors, government partners, and law enforcement on a continuous basis through public-private initiatives such as the CSCSWG and the DHS-led Cyber UCG to share information and to collaborate on incident response.

Additionally, the HPH Sector leverages key capabilities provided by the HITRUST organization to enhance the Sector's cybersecurity posture. HITRUST maintains a widely adopted cybersecurity and privacy information risk and compliance management framework (HITRUST CMF) for the HPH Sector that fully incorporates the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*[24] and provides for 135 individual security controls and 14 individual privacy controls. HITRUST, in partnership with HHS, Federal Bureau of Investigation, NIST, and DHS, offers additional cyber threat warning and intelligence services (i.e., briefings, trainings and preparedness exercises) to HPH stakeholders through:

- The Cyber Threat Intelligence and Incident Coordination Center (C3) which provides industry-specific threat, intelligence sharing, and Sector-wide cyber incident coordination;
- CyberRX which conducts sector-specific cyber threat awareness exercises; and
- The Cyber Threat Exchange, an industry-wide cyber-threat early warning system offering automated "indicator of compromise" distribution services.

Finally, in the near future, the HPH Sector will engage in an important information sharing effort with the Office of the Director of National Intelligence (ODNI) as ODNI develops classified and unclassified

DHS Fusion Center and Health Security Information Sharing and Coordination Technical Assistance Workshop

To support SLTT partners, DHS provides the Fusion Center and Health Security Information Sharing and Coordination Technical Assistance workshop, designed to support fusion centers in their efforts to integrate HPH partners into existing information sharing initiatives. This workshop is a one-day facilitated discussion, provided at no cost to the requesting jurisdiction, utilizing peer-to-peer training to share best practices for strengthening public health and fusion center partnerships and implementing mechanisms to share chemical, biological, nuclear, radiological, and health-related threat information to support the Nation's health security. Requests for this workshop must be made by the fusion center, but HPH partners are encouraged to reach out to their fusion center to discuss bringing this opportunity to their jurisdiction. More information about the Technical Assistance program is available.

Figure 11: An example of effective information sharing in the HPH Sector

reports on threats to targeted entities within each critical infrastructure sector. This is an activity that will directly support the Sector's risk assessment, risk management, and information sharing goals as identified in Section 4 of this SSP.

[24] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Effective and secure information sharing is a priority of the HPH Sector. Ongoing efforts to share lessons learned and best practices among all Sector partners will contribute to enhanced critical infrastructure security and resilience. Protecting proprietary or sensitive information is essential to the success of information sharing efforts. The HPH Sector follows a comprehensive vetting process to ensure that only trusted members of the Sector are granted access to the HSIN-HPH portal. The Sector posts unclassified or FOUO information to the portal and holds periodic classified threat briefings for cleared Sector representatives. The HPH Sector also participates in the DHS Protected Critical Infrastructure Information (PCII) Program, which ensures that sensitive or proprietary data that is shared with the Federal Government in the appropriate manner and accepted as PCII is protected from disclosure via the Freedom of Information Act, SLTT disclosure laws, use in regulatory actions, and use in civil litigation.

3.10 Value Proposition

For a large, diverse services sector like the HPH Sector, the NIPP public-private partnership structure is a primary means to allow government and private sector partners to work together to improve security and resilience and reduce risk. Participation in this partnership model provides many advantages, including:

- Access to actionable and timely threat information;
- An avenue for information exchange between the Federal Government and other sector partners;
- Networking opportunities to build community contacts in advance of potential threats and incidents;
- Access to sector risk management planning activities;
- Advanced planning for resilience and restoration of disrupted services;
- Staying connected and informed about what is going on in the Sector;
- Real-time incident management collaboration and coordination;
- Opportunities to share best practices between community members;
- Opportunities to benchmark against other participating organizations;
- Ability to inform government actions and policies;
- Ability to leverage exercises, tools, resources, and Sector WG to meet specific security and resilience building needs; and
- Public recognition for preparedness, continuity of service, and corporate citizenship.

4 Vision, Mission, Goals, and Priorities

The strategic direction for efforts to enhance and sustain the security and resilience of HPH Sector critical infrastructure is informed by the common vision and mission detailed in the NIPP 2013, as well as by the NIPP's Call to Action and the Joint National Priorities established by the NIPP Sector Councils. Taking into account this overarching guidance, the HPH Sector partnership has set its Sector-specific vision, mission, goals, and priorities while considering resource availability, progress already made, known capability gaps, and emerging risks.

Over the next four years, this strategic direction will help drive collective action broadly across the Sector, as further tailored to meet specific subsector, regional, SLTT government, and private sector partner considerations.

4.1 Sector Partnership Vision

A public-private partnership supporting the needs of HPH critical infrastructure and FSLTT government partners to enhance security and resilience of the Sector to all hazards.

4.2 Sector Partnership Mission

To sustain the essential functions of the Nation's healthcare and public health system and to support effective emergency preparedness and response to nationally significant hazards. Public and private sector partners will evaluate risks; coordinate plans and policy advice; and provide guidance to prevent, protect, mitigate, respond to, and recover from all hazards faced by the Nation's HPH critical infrastructure.

4.3 Goals and Priorities

The NIPP 2013 describes a shared vision in which physical and cyber critical infrastructure remain secure and resilient while vulnerabilities are reduced, potential impacts of incidents are minimized, threats are promptly identified and addressed, and response and recovery efforts are hastened. The goals outlined in the NIPP 2013 reflect expected outcomes from a proactive and inclusive partnership among all levels of government and the private sector. Existing capabilities will be leveraged and new capabilities will be developed to strengthen security and resilience by more effectively assessing and managing risks and enhancing preparedness. In a complementary fashion, the HPH Sector has developed a set of five Sector-specific goals and nine near-term priorities to help implement the Sector's overarching vision and mission. The goals and near-term priorities presented in Table 2 are intended to guide resilience-building activities and investments; they will be periodically reviewed by the SCC and GCC leadership and will evolve in response to new policies, challenges, and threats over the period of this SSP.

Table 2: HPH Sector Goals and Priorities. This table lists the goals and near-term priorities of the HPH Sector.

HPH Sector	Goals	Near-Term Priorities
Risk Assessment	Leverage relationships and resources to assess and analyze threats to, vulnerabilities of, and consequences of disruption to HPH Sector critical infrastructure to inform risk management activities. Ensure that approaches consider the physical, cyber, and human elements of critical infrastructure security and resilience, supply chain issues, and interdependencies with other sectors.	Plan and execute a risk assessment methodology to assess the risks of physical, cyber, and human vulnerabilities and threats in the Sector. **Implementation Lead: RMWG**
Risk Management	Enhance resilience of the HPH Sector by translating risk analyses into actionable recommendations for SLTT public health departments, private sector facilities, and health systems at large, and integrating such risk analyses into other mitigation, response, and recovery efforts of the Federal Government. Execute risk mitigation activities in a prioritized manner with clear plans and metrics for success.	Develop a long-term risk mitigation plan and set priorities based on a Sector risk assessment, leveraging existing products developed by partners, healthcare trend analyses, and needs of critical infrastructure owners and operators. **Implementation Lead: A&I WG** Develop guidance, in coordination with DHS, for Sector implementation of the NIST Cybersecurity Framework. **Implementation Lead: Cybersecurity WG**
Information Sharing	Enhance existing and develop new mechanisms to ensure bidirectional sharing of information. Promote sharing of risk information, threats, best practices, and lessons learned between government and private sector partners.	Assess the effectiveness of current processes, mechanisms, and systems used to share information among Sector partners. **Implementation Lead: A&I WG** Strengthen the dialogue between government and private sector partners about the challenges and benefits of two-way information sharing, particularly with respect to what can be shared, and cybersecurity incidents and gaps. **Implementation Lead: Cybersecurity WG**

HPH Sector	Goals	Near-Term Priorities
Partnership Development and Coordination	Develop and implement a "Partnership Engagement Strategy" to include outreach efforts to both government and private sector entities, with a focus on developing relationships with owners and operators of critical infrastructure. Encourage development of regional, SLTT, cross-sector, and intra-HPH Sector partnerships to enhance sector resilience, facilitate information sharing, and response to disasters.	Develop a "Partnership Engagement Strategy" that enhances existing and develops new outreach material, and determines key partners that are not currently engaged in SCC/GCC activities. **Implementation Leads: SCC/GCC Leadership; A&I WG** Analyze and broaden partnerships to support critical infrastructure security and resilience and to better understand the relationship between HPH critical infrastructure and community resilience. **Implementation Leads: SCC/GCC Leadership; A&I WG**
Response and Recovery	Engage in HPH response and recovery efforts across FSLTT governments, health care coalitions, and the private sector during and after disasters, including cybersecurity incidents. Exercise the ability of the Sector to respond to natural or manmade disasters and incorporate lessons learned into future exercises and corrective actions.	Clarify HPH response and recovery roles and functions among FSLTT governments, healthcare coalitions, and the private sector, including PPD-8 and ESF-8 activities. **Implementation Lead: SCC/GCC Leadership** Exercise the entire Sector partnership, both at the sector level and through national-level all-hazards exercises, including cyber exercises, such as Cyber Storm V. **Implementation Leads: RMWG; Cybersecurity WG**

The following are additional activities in support of HPH Sector goals that may be undertaken during the period of this SSP by the GCC and SCC. All activities are subject to review and revision, and additional activities may be considered for inclusion throughout the time period covered by this SSP.

Risk Assessment

- Utilize risk assessments to identify risks to specific infrastructure and systems and broaden results to create general considerations for the Sector at large.
- Consider lifeline sector dependencies and interdependencies, healthcare trends—such as technological advances, personalized medicine, electronic health records, and other Affordable Care Act innovations—and community health resilience.
- Pursuant to E.O. 13636 (Sec. 4a), support the ODNI in the development and issuance of unclassified reports of cyber threats to the U.S. homeland that identify specifically targeted HPH Sector entities; information gleaned will be utilized to inform Sector risk management activities.
- Review and update lists of HPH critical infrastructure, including cyber assets.
- Work with the intelligence community to better understand the threats to the HPH Sector and develop plans to receive timely and actionable information relevant to the Sector.
- Educate public and private sector partners about Sector threats.

Risk Management

- Connect with owners and operators of critical infrastructure to develop a Sector risk mitigation plan and assist in its implementation.
- Provide training materials and informational products to help the HPH Sector better understands risks and how to better communicate risks to Sector leaders, the workforce, and surrounding communities.
- Identify strategies for enhancing the resilience of supply chain networks.

Information Sharing

- Optimize current communication mechanisms, including (but not limited to) HSIN, HHS CIP public-facing websites, and the text messaging program, which are the Sector's means for supporting information sharing relevant to all hazards.
- Identify and address barriers to sharing information.
  - Educate the Sector on the sharing of PCII.
  - Support partner efforts such as the Nationwide Suspicious Activity Reporting Initiative and Fusion Centers.
- Provide a framework for how cyber information (including threats, vulnerabilities, and mitigation measures) can be shared between the private sector and the Federal Government.
- Connect with owners and operators of critical infrastructure to better understand Sector partners' needs across all levels of government (e.g. local HPH organizations), and to develop methods to share relevant, timely, and actionable information in accordance with those needs.

Partnership Development and Coordination

- Develop a partnership engagement strategy.
  - Enhance connections to owners and operators of critical infrastructure, SLTT Government Coordinating Council, NIPP cross-sector councils, and other sectors.
    - Bring additional cyber experts to the partnership from the public and private sectors.
    - Expand the annual in-person GCC-SCC Joint Meeting to include more partners, such as owners and operators of critical infrastructure, FSLTT entities, and professional associations that play a role in response.
- Explore the extension of the HPH Sector via regional resilience coalitions and organizations, such as the Bay Area Center for Regional Disaster Resilience.
- Continuing on the success of the joint DHS-HPH Cybersecurity Workshop held in October 2014, partner with DHS CS&C, as needed, to augment cybersecurity efforts, risk awareness, and stakeholder outreach.
- Enhance partnerships with academia, including the new Critical Infrastructure Security and Resilience Center of Excellence at the University of Illinois.
- Recognize the importance of healthcare coalitions and incorporate them into the HPH Sector partnership structure.
- Enhance relationships between the Sector, infrastructure owners and operators, and Federal regional staff, such as DHS Protective Security Advisors, ASPR Regional Emergency Coordinators, and HHS and FEMA grants coordination staff, as appropriate.
- Improve and enhance the Sector's partnership communication strategy.
  - Develop membership welcome materials, including a compilation of benefits to joining the SCC and GCC.
  - Clarify the goal of HSIN and the role of its members who are not part of the SCC.

Response and Recovery

- Optimize information collection during disasters through DHS, HHS, NICC, and/or the Incident Command System.
- Support continuity of operations planning for the Sector; involve lifeline sectors, communications, workforce planning, etc.
- Develop a cyber concept of operations to explain the actions taken if a private sector entity reports a breach or cyberattack. Ensure resources for planning, response, and recovery--such as clearances, the Wireless Priority Service, Government Emergency Telecommunications Service (GETS), and C³ Voluntary Program resources--are available to Sector partners to prepare for disaster response.
- Provide education to private sector partners to explain public sector response plans, including communications during a disaster.
- Develop a liaison program to encourage private sector participation in exercises and response operations.
- Connect HPH Sector members with local responders.
- Highlight Suspicious Activity Reporting efforts.
- Strengthen the Sector's ability to coordinate internally on sharing cyber threats and responding to incidents that impact the public and private sector.
- Develop resources to assist private sector partners in navigating requirements of various crisis re-entry credentialing programs across the country.

4.4 Mapping to the National Infrastructure Protection Plan 2013 Call to Action

The NIPP 2013 establishes a Call to Action and supporting national activities to guide efforts to collaboratively attain national goals via the NIPP partnership model. Collectively, these activities are intended to serve as a roadmap to guide national progress while allowing for the development of supporting customized priorities within the various critical infrastructure sectors. Sector-level goals and priorities supporting this National Call to Action are to be developed and implemented with a tailored approach, taking into consideration the unique risk management perspectives, priorities, and resource constraints of each sector. The NIPP Call to Action activities are identified in Figure 12.

The relationships between the NIPP 2013 Call to Action activities and the HPH Sector goals and priorities established in this SSP are depicted in Appendix A.

NIPP 2013 Call to Action Activities

Build upon Partnership Efforts:

1. Set National Focus through Jointly Developed Priorities
2. Determine Collective Actions through Joint Planning Efforts
3. Empower Local and Regional Partnerships to Build Capacity Nationally
4. Leverage Incentives to Advance Security and Resilience

Innovate in Managing Risk:

1. Enable Risk-Informed Decision-Making through Enhanced Situational Awareness
2. Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects
3. Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents
4. Promote Infrastructure, Community, and Regional Recovery Following Incidents
5. Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education
6. Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions

Focus on Outcomes:

1. Evaluate Progress toward the Achievement of Goals
2. Learn and Adapt During and After Exercises and Incidents

Figure 12: NIPP Call to Action activities

4.5 Aligning with the Joint National Priorities

The first Call to Action activity identified in the NIPP 2013 involves the setting of joint, multi-year priorities for the NIPP partnership and their subsequent annual review on the part of the NIPP Sector Council structure with input from all levels of the critical infrastructure community. These priorities are to take into account an evaluation of existing and emerging risks, known capability gaps, resource availability, best practices, etc., across all levels of the NIPP partnership. The Joint National Priorities are intended to focus partner efforts as they implement activities to accomplish the remaining NIPP calls to action, develop and implement updated SSPs, and pursue related efforts in support of the NIPP 2013 strategic goals. While these Joint National Priorities provide a common focal point for partnership efforts, critical infrastructure partners at the Sector-level are to continue to share information and implement a variety of security and resilience activities, as appropriate to their unique risk and operating environments. The NIPP Joint National Priorities are identified in Figure 13.

NIPP Partnership Joint National Priorities for 2014-2015

1. Strengthen the Management of Cyber and Physical Risks to Critical Infrastructure
2. Build Capabilities and Coordination for Enhanced Incident Response and Recovery
3. Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines
4. Enhance Effectiveness in Resilience Decision-Making
5. Share Information To Improve Prevention, Protection, Mitigation, Response, and Recovery Activities

Figure 13: NIPP Partnership Joint National Priorities

The relationships between the NIPP Partnership Joint National Priorities for 2015 and the HPH Sector goals and priorities established in this SSP are depicted in Appendix B.

5 Achieving Sector Goals: Sector Activities and National Preparedness

The importance of the HPH Sector is exemplified by its size and its span to nearly every community in America. The range of risks to the HPH Sector critical infrastructure is as diverse and far-reaching as the Sector itself. Every region of the U.S. in which HPH assets can be found is subject to different types of threats to people and infrastructure, including extreme weather events and multiple forms of manmade threats, from terrorist attacks to supply chain disruptions. To confront this challenge, the HPH Sector is committed to refining and implementing a strong risk management approach with participation from and engagement between all Sector partners.

Identified by the NIPP 2013 as the cornerstone of critical infrastructure security and resilience, the HPH Sector utilizes the NIPP Risk Management Framework as the basis for the Sector's strategic approach to addressing risk to critical infrastructure across its physical, cyber, and human dimensions.

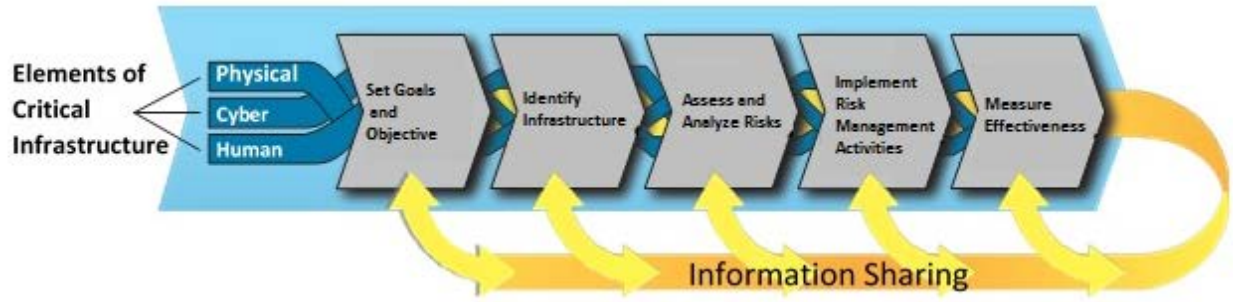
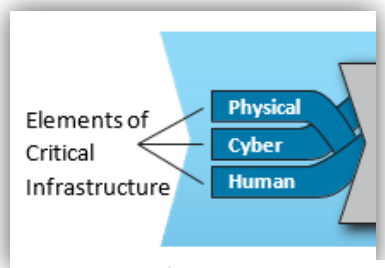


Figure 14: NIPP 2013 Risk Management Framework

The NIPP Risk Management Framework (Figure 14) is designed to support the critical infrastructure community in identifying and prioritizing each sector's critical components and key internal and external dependencies and interdependencies; defining the threats and hazards most likely to cause harm or disruption of services; and employing prioritized approaches to prevent, protect against, and/or mitigate the effects of those threats and hazards. It also increases security and strengthens resilience by identifying and prioritizing actions to ensure continuity of essential functions and services and support enhanced response and restoration in the context of incidents in progress. The five steps of the NIPP Risk Management Framework are: Set Goals and Objectives; Identify Infrastructure; Assess and Analyze Risks; Implement Risk Management Activities; and Measure Effectiveness. The three elements of critical infrastructure (physical, cyber, and human) span this framework and should be integrated through a comprehensive risk management approach. A continuous loop of information is shared at each step of the process to facilitate feedback and enable continuous improvement of critical infrastructure security and resiliency efforts.



This excerpt from Figure 14 highlights the interconnected physical, cyber, and human elements of infrastructure.

The Sector's risk management approach is informed by a number of important updates to the Risk Management Framework provided in the NIPP 2013.

First, the three elements of critical infrastructure (physical, cyber, human) are explicitly identified in order to encourage full consideration of each in every step of the framework. Human threats to the

sector encompass a wide array of potential threat actors ranging from disaffected employees, to active shooters, to domestic and international terrorist organizations. Facilities comprising the HPH Sector include a geographically distributed array of physical assets and supporting infrastructure that can be impacted by a number of complex manmade and naturally occurring threats and hazards. Finally, in the context of cyber, the HPH Sector is increasingly dependent upon interconnected information technology systems, including Health IT. The protection of the systems used to provide care, maintain patient records, store intellectual property, and perform financial operations is extremely challenging and important. A failure anywhere in this complex environment can have immediate cascading consequences across the Sector.

This excerpt from Figure 14 highlights the fact that prioritization is a key consideration within each step of the NIPP Risk Management Framework.

Secondly, "Prioritization" now is considered as a component of each individual step of the NIPP Risk Management Framework. Prioritization is a critical part of risk decision-making in the HPH Sector because of the number and type of assets, risks, and resource limitations the Sector has to consider.

Thirdly, former reference to the "feedback loop" has been replaced with the arrow graphic, depicting the importance of information sharing throughout the entire risk management process. In a sector that includes over 14 million workers and a large number of diverse facilities and supporting systems, individuals and organizations have varying perspectives on risk management based on diverse commitments, business plans, resources, operating structures, regulatory requirements, etc. Taking this into account, partnership and the sharing of information across HPH Sector entities are essential to improving the understanding of threats, vulnerabilities, and consequences, as well as for providing Sector partners—including owners and operators—with tools, guidelines, information, best practices, and resources to facilitate more effective risk management across the Sector. The principal information sharing mechanisms used by the HPH Sector are discussed above in Section 3 of this SSP.

This excerpt from Figure 14 highlights that information sharing spans the individual steps of the NIPP Risk Management Framework.

5.1 Risk Management

While individual organizations within the HPH Sector are responsible for managing risk to their own infrastructure assets, systems, and networks, a collective approach can improve understanding of threats, vulnerabilities, and consequences. Effective partnership can also provide Sector partners with tools, guidelines, information, best practices, and resources to facilitate more effective risk assessments and risk management decisions at the Sector and individual asset levels. This section presents the HPH Sector's efforts to employ the NIPP Risk Management Framework to mitigate threats, hazards, and vulnerabilities, and to better support national preparedness, response, and recovery capabilities on a sector-wide basis.

5.2 Set Goals and Objectives

As the first step in the risk management process, the HPH Sector has established a number of goals and affiliated priorities (described in Section 4 above) that support the National Call to Action laid out in the NIPP 2013. These goals and priorities provide the foundation for the Sector's voluntary and collaborative efforts to address its risk profile and improve the security and resilience of its identified critical infrastructure over the next four-year SSP implementation cycle. The goals and priorities also reflect the maturation of the partnership and the significant progress made since the issuance of the previous HPH SSP in 2010.

5.3 Identify Assets

The HPH Sector participates in the DHS National Critical Infrastructure Prioritization Program (NCIPP), the goal of which is to identify and prioritize critical infrastructure with national level significance across the 16 critical infrastructure sectors. DHS issues an annual data call to sector and State and territorial government partners, using criteria developed by the DHS OCIA.[25] OCIA uses a tiered approach to identify a prioritized list of nationally significant critical infrastructure. This identifies assets and systems (Levels 1 & 2) critical to the national effort to protect infrastructure and mitigate risks. These lists are consequence-based, referring to the effect of an event on public health and safety, national security, national economic security, and continuity of essential services. Through the annual data call process, DHS also works with State Homeland Security Advisors (HSAs) and the RMWG, assisting them in the creation and submission of Sector- and State-level lists of critical assets (Levels 3 & 4, respectively). The HPH SSA assists in the process by working with State public health agencies, providing them the tools and supplemental information needed to identify HPH-related infrastructure in coordination with their State HSAs. The NCIPP data collection process is illustrated in Figure 15.

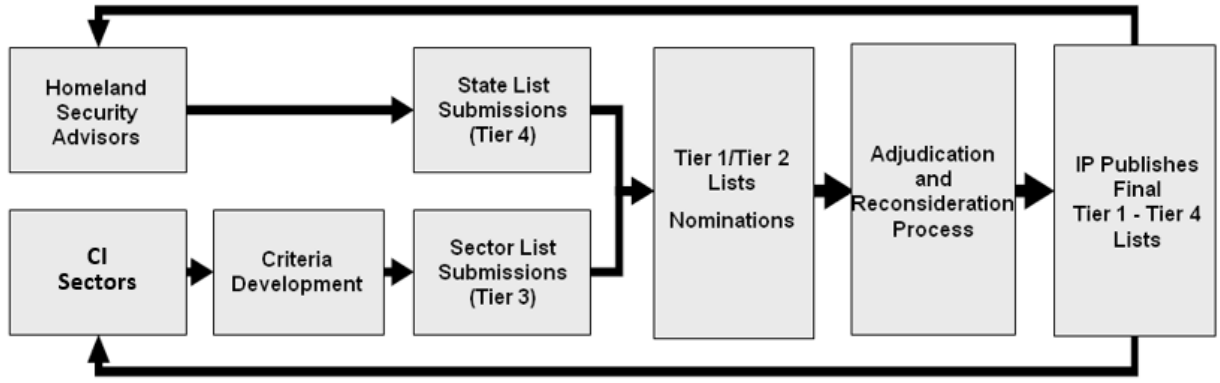


Figure 15: DHS Data Collection Process for DHS IP Tier Lists

5.4 Prioritize Assets

The HPH Sector identifies and prioritizes its critical assets and participates in the NCIPP data call through the efforts of the RMWG. Figure 16 identifies key goals identified in the RMWG Charter. Comprised of experts from across the Sector, the RMWG is responsible for developing and refining the Sector's critical infrastructure identification criteria. Using these criteria, the RMWG analyzes critical functions in the

[25] In February 2014, the DHS National Protection and Programs Directorate (NPPD) created the Office of Cyber and Infrastructure Analysis by integrating analytic resources from across NPPD including the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and the National Infrastructure Simulation and Analysis Center (NISAC).

Sector that, if disrupted, would lead to overall mission degradation and unacceptable cascading consequences. The RMWG then identifies asset types and, subsequently, the specific assets that support critical functions within the Sector as well as their associated attributes. Following the issuance of the 2010 SSP, the RMWG led a major analysis of the Sector's critical infrastructure that resulted in a new Sector list in 2012.

Figure 16: Risk Management Working Group (RMWG) Goals

In an effort to provide the most accurate and reliable list of critical infrastructure assets possible, the HPH Sector has recently undertaken a review of its existing asset identification methodology, ensuring enhancements to the methodology will be incorporated into an updated HPH Sector asset identification methodology to be completed and implemented in 2017.

The HPH Sector also participates in the identification and prioritization of critical cyber-dependent infrastructure. In 2013, DHS was tasked with carrying out the responsibilities necessary to implement Section 9 of E.O. 13636, *Improving Critical Infrastructure Cybersecurity*. To accomplish this task, DHS used a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. The HPH Sector will continue to work with DHS to provide ongoing review of HPH Sector critical cybersecurity functions and services as part of the Cyber-Dependent Infrastructure Identification effort mandated in E.O. 13636. The HPH Sector will incorporate cyber-dependent asset identification into the 2017 Critical Asset Identification Process review process.

Identification supports both critical infrastructure needs and national security objectives by:

- Providing the Federal Government with the ability to more effectively disseminate specific and targeted cybersecurity threat information to identified cyber dependent critical infrastructure owners and operators;
- Supporting the prioritization, as appropriate, of government resources and programs available to identified cyber-dependent critical infrastructure; and
- Improving the government's understanding of the systems or assets whose incapacity or disruption would result in catastrophic loss of life or significant monetary consequences or would adversely impact government planning, protection, mitigation, and response efforts provided in partnership with impacted SLTT and private sector entities in the event of a cyber incident.

5.5 Assess and Analyze Risk

The NIPP 2013 defines risk as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. Risk is influenced by the nature and magnitude of a threat or hazard, the vulnerabilities to that threat or hazard, and the ensuing consequences. Risk assessment information allows partners, from facility owners and operators to Federal agencies, to prioritize risk management efforts.

Generally speaking, individual organizations within the Sector perform risk assessments for their own critical assets. Due to the diversity of the HPH Sector, specific risk assessment methodologies may vary from failure modes and effects analyses to hazard and operability studies. These methodologies may be used to determine risk to specific facilities, systems, supply chains, or other discrete components of the Sector's infrastructure. They may also serve to highlight the importance of key internal interdependencies as well as dependencies on other sectors. To support the efforts of individual organizations within the Sector to analyze risks and identify dependencies and interdependencies, the HPH SSA and its GCC and SCC partners work to employ a variety of mechanisms to better identify and

Threat-Related Suspicious Activity Reporting

In FY 2016, the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), in partnership with DHS and HHS, will develop and deploy sector-based training for HPH partners on indicators of suspicious activities. The everyday duties and responsibilities of HPH professionals, such as treating patients for medical conditions, talking to community members, conducting inspections, or monitoring disease trends in a community, place them in a unique position to observe suspicious behaviors and indicators that, when viewed in the context of other facts and circumstances, may indicate preoperational planning of a terrorist-related incident or other criminal activity. Given their positions of trust with their patients, healthcare professionals also have the unique responsibility to balance the obligation to report suspicious activity with the obligation to protect patient privacy. The NSI training will assist public health and healthcare professionals in recognizing what kinds of suspicious behaviors are associated with pre-incident terrorism activities, understanding how and where to report suspicious activity, and protecting privacy, civil rights, and civil liberties when sharing the information. The integration of HPH professionals into this partnership of FSLTT officials for gathering, analyzing, and sharing suspicious activity information can help to connect the dots in order to prevent, protect against, and respond to threats to the homeland. Furthermore, increased collaboration between law enforcement and public health partners through information sharing of emerging threats can enhance public health preparedness efforts, support first responder safety, and increase situational awareness for all partners. More information about the Nationwide Suspicious Activity Reporting (SAR) Initiative is available.

Figure 17: Threat-Related Suspicious Activity Reporting

communicate threats, assess vulnerabilities, and evaluate consequences to form a more accurate picture of the Sector's unique risk environment.

At the Sector level, risks are assessed as a function of threats, vulnerabilities, and consequences associated with a particular event type. Effective and reliable risk assessment is a goal of the HPH Sector and is a critical part of the Sector's underlying risk management priorities. The risk assessment process

should include participation on the part of all HPH Sector partners—owners/operators, government and Sector councils, and both government and nongovernment agencies. One example of this all-inclusive approach to risk assessment is the threat-related SAR program described in Figure 17.

The SSA and RMWG will develop an overarching risk assessment methodology that can be tailored for use at the sector and subsector level to help identify a composite risk picture, serve as an indicator of key risk trends and patterns, and help focus broad-based risk management activities. The results of this effort will be available to the Sector as a whole via lessons learned, compiled trends, and other sector-specific products or reports.

5.6 Achieving Risk Management: Sector Activities

To achieve the goals and priorities identified in Section 4 above and to address critical aspects of the HPH Sector risk profile, the Sector has developed a list of near-term priorities and additional activities to be carried out over the term of this SSP. These joint activities of the GCC and SCC are also identified in Section 4. Additional examples of ongoing activities of individual Sector partners, which ultimately contribute to Sector security and resilience, are presented below.

5.6.1.1 HPH Sector Partner Risk Management Activities

Many entities within the HPH Sector, many of which are members of the SCC and GCC, undertake independent activities which contribute to the overarching risk management aims of the Sector. The Association of Public Health Laboratories provides one important example. To promote critical infrastructure security and resilience, it educated its members on ways to enhance laboratory biosafety and biosecurity by holding multiple seminars on these topics in 2015. Biosafety and biosecurity are both vital components of public health as an accident, breach, or failure in either area could lead to dangerous exposure to infectious agents.

Many HPH organizations, such as Kaiser Permanente, the Washington Hospital Healthcare System, and the Department of Veterans Affairs (VA) are helping to enhance the security and resilience of the HPH Sector by upgrading their physical infrastructure assets. Rather than retrofitting and upgrading older buildings in a patchwork manner, Kaiser Permanente has completely replaced twelve of its California hospitals since 2007. The new hospitals are designed to remain both intact and functional following a major earthquake. The Washington Hospital Healthcare System built a new "critical care pavilion" which houses an emergency department four times larger than the previous one, as well as a state-of-the-art intensive care unit, and an advanced coronary care unit. When a VA hospital was destroyed by Hurricane Katrina, the Department decided to set a new standard for storm-ready healthcare facilities with its replacement. Innovative aspects of the new VA hospital include situating sensitive patients and operations on upper floors, and a boat dock for receiving patients and supplies during a flood. These new buildings and their enhanced design features will play an important role in future HPH Sector resilience.

5.7 Sector Cybersecurity Efforts

The NIPP Risk Management Framework identifies cyber as a critical infrastructure element to be protected in every sector. Likewise, E.O. 13636 calls for improved cybersecurity information sharing and the collaborative development and implementation of risk-based approaches to cybersecurity. E.O.

13636 also requires the NIST to work with stakeholders to develop a voluntary framework—based on existing standards, guidelines, and practices—for reducing cyber risks to critical infrastructure. The relationship between HPH Sector risk management activities and the final NIST Cybersecurity Framework is highlighted in Appendix C. In addition to the NIST Cybersecurity Framework, this SSP also directly supports the Nationwide Interoperability Roadmap, released by the Office of the National Coordinator (ONC) for Health Information Technology, which contains critical actions, such as ONC coordination with ASPR on priority issues related to cybersecurity for critical public health infrastructure. Most recently, the White House issued E.O. 13691, *Improving Private Sector Information Sharing*, to encourage and promote the sharing of cybersecurity threat information within the private sector and between the private sector and government. This Executive Order lays out a framework for expanded information sharing designed to help private sector entities work together, as well as with the Federal Government, to more quickly identify and protect against cyber threats.

The importance of effective cybersecurity measures is especially clear based on several recent, major HPH Sector cyber breaches which affected several million patient records based on HPH Sector and NH-ISAC reporting. The total number of patient records affected across all five recent breaches was more than 90 million, in addition to numerous smaller breaches of other HPH Sector organizations over the same time period. These breaches affected the Direct Patient Care and Health Plans and Payers Subsectors and were larger than any other breach reported in the Sector's history. The breaches were announced over the span of just nine months.

The HPH Sector takes a collaborative approach to cyber risk by working with DHS CS&C to evaluate cybersecurity threats, vulnerabilities, and consequences related to critical functions to establish and address the Sector's cyber risk management priorities. The Sector's cyber risk assessment and prioritization process also builds on several additional partnership activities:

- Efforts in collaboration with DHS CS&C to support the Critical Infrastructure Cyber Community (C³) Voluntary Program,[26] which serves as the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes. The program supports Sector partners in increasing cyber resilience and the Sector's awareness and use of the NIST *Framework for Improving Critical Infrastructure Cybersecurity.*
- Identification and ongoing review of HPH Sector critical cybersecurity functions and services as part of the Cyber-Dependent Infrastructure Identification effort mandated in E.O. 13636. This effort identified Sector critical functions that were validated by Sector subject matter experts.
- Incorporation of cybersecurity considerations as part of the Sector Risk Assessment Methodology effort described in Section 5.1.4 to help inform sector-specific risk management strategies and decision-making and to provide a linkage between national and organizational cyber risk management efforts.
- Establishment of a joint GCC-SCC WG to focus on preparedness and response to cyber threats across the Sector.

[26] For more information regarding the Critical Infrastructure Cyber Community Voluntary Program, please see the CERT website.

- Expansion of cybersecurity expert participation in the HPH Sector partnership and expanded focus on cybersecurity information sharing—including threat, response, mitigation, and remediation information—among Sector partners through the services provided by ISACs and ISAOs such as the NH-ISAC and HITRUST.
- Development of guidance, in coordination with DHS, for sector-specific tailoring and implementation of the NIST Cybersecurity Framework.
- Collaboration with members of the Health Information Technology Subsector to coordinate the Sector's implementation of E.O. 13691, *Improving Private Sector Information Sharing.*
- Development of a cyber concept of operations (CONOPS) to explain the actions taken if a private sector entity reports a breach or cyber attack. This cyber CONOPS will address how HHS (in its SSA role) coordinates and collaborates with industry and Federal partners via incident management, information sharing, and cybersecurity efforts.
- Coordination and encouragement of Sector participation in planning and conducting the Cyber Storm exercise series.
- Pursuant to E.O. 13636 (Sec. 4a), support the ODNI in the development and issuance of unclassified reports of cyber threats to the U.S. homeland that identify specific targeted HPH Sector entities.

5.8 Sector Research and Development Priorities

Ongoing R&D activities are essential for developing new methods and tools to improve critical infrastructure security and resilience, both nationally and at a sector level. With this in mind, PPD-21 directed the Federal Government to develop an R&D plan that accounts for the evolving threat landscape, annual metrics, and other relevant information to identify priorities and guide R&D requirements and investments. The resulting *National Critical Infrastructure Security and Resilience R&D Plan* identifies the following R&D priorities for the critical infrastructure security and resilience mission area:

- Develop the foundational understanding of critical infrastructure systems and systems dynamics;
- Develop integrated and scalable risk-assessment and risk management approaches;
- Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure;
- Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action; and
- Build a cross-cutting culture of critical infrastructure security and resilience research and development collaboration.

The HPH Sector will work closely with DHS, as well as its public-private partners in the other critical sectors, to support plan implementation and ensure appropriate input from the HPH Sector as individual *National Critical Infrastructure Security and Resilience R&D Plan* projects are developed and conducted. Additionally, the SSA will work continuously with Sector partners to identify and inform them of the latest developments in the Sector's R&D portfolio, as well as out-of-sector R&D activities that may be of

ongoing interest. These activities will be identified and updated on the SSA's CIP Office website. Sector partners are encouraged to provide inputs on R&D activities taking place at their level that may have broader Sector applicability.

5.9 Managing Risk during an Incident: Critical Infrastructure Security and Resilience and National Preparedness

PPD-8 identifies national preparedness as the shared responsibility of all levels of government, the private and nonprofit sectors, and individual residents. The HPH Sector is responsible for ensuring that its critical infrastructure security and resilience activities are integrated with the overarching National Preparedness System created by PPD-8. As called for in the NPG, the Sector is similarly responsible for building out the core capabilities necessary to prepare for incidents that pose the greatest risks to the Nation's security, including those that may threaten or otherwise impact Sector critical infrastructure. The 31 core capabilities identified in the NPG are strategic in nature to ensure that they comprehensively include and mutually support all five preparedness mission areas: prevention, protection, mitigation, response, and recovery. The HPH Sector must be prepared to address all five mission areas in order to fulfill its national responsibilities, as well as its Sector risk management goals.

To guide the Sector's activities in support of PPD-8, the NHSS drives actions that communities must take to address each key mission area. Further, the HPH Sector, through the HHS ASPR and CDC, and their respective partners, has developed State and local preparedness capabilities that operationalize the PPD-8 core capabilities relevant to HPH infrastructure assets. The CDC's *Public Health Emergency Preparedness Capabilities: National Standards for State and Local Planning* and the ASPR's *Healthcare Preparedness Capabilities: National Guidance for Healthcare System Preparedness* provides guidance to assist State and local partners in the execution of core capabilities, as well as to bridge the national and Federal capabilities with corresponding SLTT actions.[27]

Responding To and Recovering From the Joplin Tornado

- All three hospitals in the area quickly activated their Incident Command Systems (ICS).
- Multiple sister hospitals of Mercy Hospital Joplin also activated their ICS and began supporting the response effort using all available resources and staff.
- Within a week, a temporary hospital was deployed to the area and made operational, filling the acute care and surgical void left when Mercy Hospital was destroyed.
- Less than nine months after the tornado hit, Mercy Hospital opened a component hospital made of steel and concrete, expanding the local healthcare options to make available more complicated operations, such as open heart surgery and labor and delivery, and increasing the number of available beds to 120.
- A new $465 million hospital opened in 2015 and is designed to withstand an EF3 tornado (the maximum expected magnitude since EF5 is a rare event). It boasts reinforced shelter areas, extra underground power and water connections, and sufficient generator capability to sustain operations for four days.

Figure 18: The HPH Sector response to the tornado in Joplin, MO [28, 29,30]

[27] For additional information on how the HPH Sector is aligned with PPD-8, please refer to the NHSS.

Finally, as a key component of any emergency response operation, the HPH Sector must be prepared to transition from steady state to incident response and recovery using the National Response Framework's ESFs and the National Disaster Recovery Framework's Recovery Support Functions (RSFs). This principle of rapid transition aligns closely with the fourth strategic objective of the NHSS: enhance the integration and effectiveness of the public health, healthcare, and emergency management systems. This objective directs organizations to build on and improve routine services and systems as a foundation for incident response and risk reduction, focusing on common elements that leverage the alignment of routine capabilities with those needed during an incident. Figure 18 provides an example of a coordinated and effective response and recovery effort undertaken by the HPH Sector in the aftermath of a catastrophic natural disaster event. [28,29,30]

There are 15 ESFs designed to group government and certain private sector capabilities into recognized organizational structures to provide support, resources, program implementation, and services that are most likely to be needed to save lives, protect property and the environment, restore essential services and critical infrastructure, and help victims return to normal life after domestic incidents and disasters. HHS is the lead agency for ESF-8, Public Health and Medical Services, which coordinates resources in response to:

- Public health and medical care needs;
- Veterinary and/or animal health issues in coordination with the U.S. Department of Agriculture;
- Medical surge;
- A mass fatality situation;
- Potential or actual incidents of national significance; and/or
- A developing potential health and medical situation.

In addition to ESF-8 response activities, all incidents rely on closely coordinated local response. HPH Sector members utilize the National Incident Management System (NIMS) and the NIMS Incident Command System (ICS) to coordinate activities between government, private sector, and nongovernmental organizations. Key components of disaster response are local and regional healthcare coalitions. As hospitals struggle to meet increased demand with stagnant or diminishing resources, many regions and communities are relying more heavily on healthcare coalitions to support individual hospitals and healthcare facilities. Figure 19 explains the role and importance of healthcare coalitions.

The NIMS provides a national template for governments, communities, and the private sector to work together to implement the PPD-8 goals of preparing for, preventing, responding to, and recovering from

[28] The White House, National Action Plan for Combating Antibiotic-Resistant Bacteria, March 2015, https://www.whitehouse.gov/sites/default/files/docs/national_action_plan_for_combating_antibotic-resistant_bacteria.pdf

[29] The White House. Joplin: One Year Later, https://www.whitehouse.gov/joplin; Centers for Disease Control and Prevention, Tornado Survivors Battle Deadly Fungus in Joplin, Missouri (August 1, 2011), http://blogs.cdc.gov/publichealthmatters/2011/08/tornado/

[30] Adalja, Watson, Bouri, Minton, Morhard, and Toner. Absorbing Citywide Patient Surge During Hurricane Sandy: A Case Study in Accommodating Multiple Hospital Evacuations. *Annals of Emergency Medicine* (2014); Treperman. Hurricane Sandy and the greater New York health care system. *Journal of Trauma and Acute Care Surgery* (2013).

domestic incidents. The NIMS is scalable and adaptable to all hazards. Implementing the NIMS promotes interoperability between public and private sectors and provides the framework for the ICS.

The Role of Healthcare Coalitions in Disaster Response

Healthcare coalitions organize individual healthcare assets into a single functional unit. In a major medical response, their goal is to maximize limited medical resources through cooperative planning, information sharing, management coordination, and mutual aid. Healthcare coalitions ensure that public health and medical assets have what they need to support disaster response. In addition to hospitals, coalitions may include long-term care or alternative treatment facilities, dialysis and other outpatient treatment centers, nursing homes and other skilled nursing facilities, private physician offices, clinics, community health centers, local public health departments, and any other healthcare asset that may be brought to bear during a major medical response.

Figure 19: Role of Healthcare Coalitions in Disaster Response

ICS is a management system designed to integrate facilities, equipment, personnel, procedures, and communications operating within a common organizational structure in order to enable effective incident management. FEMA provides training for healthcare organizations to incorporate and practice the principles of ICS.[31] Since 2001, the Joint Commission for the Accreditation of Healthcare Organizations (Joint Commission) has required members to develop all-hazards, comprehensive emergency management programs and to use the ICS. Healthcare facilities receiving Federal preparedness and response grants, contracts, or cooperative agreements, must implement certain aspects of NIMS including conducting planning for the establishment of ICS structure appropriate for HPH emergency response operations.[32]

[31] Training can be found on the FEMA EMI Website: https://training.fema.gov/is/courseoverview.aspx?code=is-200.hca
[32] Joint Commission Hospital Incident Command System Guidebook, 5th Edition

6 Measuring Effectiveness

Measuring performance against established goals and priorities is a critical step in the NIPP 2013 risk management process. Performance measurement involves the objective and, where possible, quantifiable tracking of progress and the assessment of improvement in infrastructure security and resilience at both the sector and national levels. Performance metrics, in turn, provide a basis for the SSA and its GCC and SCC partners to establish accountability, document actual performance, facilitate diagnoses, promote effective risk management, and provide a feedback mechanism to decision-makers.

Over the next four years, the HPH Sector will evaluate the implementation and effectiveness of its risk management efforts based on the specific risk management activities identified in Section 4 of this SSP. Accordingly, the HPH GCC and SCC will work collaboratively to develop and/or enhance performance metrics that support both national goals and priorities and HPH Sector-specific goals and priorities. The SSA will be responsible for reporting Sector progress through the NIPP National Annual Reporting process, quadrennial SSP updates, and other means as required.

6.1 Sector Critical Infrastructure Security and Resilience Programs

In alignment with the NIPP 2013, HPH Sector goals and priorities, and the NIST Cybersecurity Framework, the HPH GCC and SCC have established performance goals that determine the activities that will be pursued to advance critical infrastructure security and resilience within the Sector. Those activities are detailed in Section 4 of this SSP; each is aligned with a Sector goal that maps to the NIPP 2013 Call to Action and the Joint National Priorities identified in Appendices A and B.

6.2 Measurement Approach

Individual entities within the HPH Sector, including private sector owners and operators, implement internal risk assessment and management processes and use a variety of methods to measure individual progress toward improving critical infrastructure security and resilience. Progress of these organizational efforts is difficult to capture and measure uniformly; hence, the SSA will focus on developing metrics and measuring progress at the sector-level against the Sector risk management activities detailed in Section 4.

6.3 Preparedness Activities, Best Practices, and Lessons Learned

In addition to the evaluation of Sector goals through formal performance metrics, planned exercises and real-world incident response activities also provide opportunities to evaluate Sector progress and for learning and adaptation throughout the Sector. The HPH Sector joins the critical infrastructure and national preparedness communities in conducting exercises on an ongoing basis through the National Exercise Program and other mechanisms to assess and validate the capabilities of Sector-specific organizations and agencies. During and after such activities, members of the HPH Sector identify capability gaps and areas in which to focus Sector risk management activities, implement and evaluate corrective actions, and share best practices with the wider critical infrastructure and emergency management communities. Similarly, real-world disasters help illustrate Sector-wide dependencies and interdependencies, the complexities of infrastructure systems, the challenges in achieving shared situational awareness during large events, and the need for improved information collection and sharing among government and private sector partners to support restoration activities.

Such learning and adaptation will inform future Sector plans, activities, technical assistance, training, and education. The HPH Sector seeks to foster an environment where public and private sector organizations can communicate about their programs and collaborate to achieve maximum effectiveness. The Sector will continue

to inform senior officials involved in policy development so that their decisions take the most critical security and resilience needs of the Sector into consideration.

6.4 Using Performance Metrics for Continuous Improvement

By using performance metrics and other forms of feedback, HPH Sector partners can adjust and adapt their approaches to account for progress achieved and changes in the threat, operational, and policy environments. At the Sector-level, metrics can be used to focus attention on areas of critical infrastructure security and resilience that warrant additional resources, plan modifications, information sharing enhancements, etc. For example, if an evaluation of the effectiveness of efforts to achieve priorities using established performance metrics reveals that there is insufficient progress, the Sector can undertake actions to focus efforts on addressing these particular gaps or launching improvement opportunities. In addition to supporting the evaluation of progress against Sector goals and priorities, metrics can also serve as a feedback mechanism for other parts of the NIPP risk management framework as applied at the sector level. For example, metrics can provide analysts with information to adjust their risk assessments or reveal the need for adjustments in sector information-sharing processes or protocols.

6.5 Performance Metrics Related to Sector Priority Activities

HHS, in coordination with HPH Sector partners, holds the primary responsibility for managing the tracking and measurement of Sector-wide progress toward achieving the goals and priorities identified in Section 4 of this SSP. HHS also coordinates data collection and reports Sector progress through the National Annual Reporting process and quadrennial SSP updates as discussed in the NIPP 2013.

In Tables 3 - 11, near-term HPH Sector priorities are aligned with proposed metrics intended to describe Sector progress, where possible. The information provided in these tables does not represent an exhaustive set of all possible metrics; rather, it is a starting point to chart specific actions and capture appropriate quantitative and qualitative feedback on the achievement of key priorities. The metrics identified in Tables 3 - 11 have been reviewed by and include input from both the HPH GCC and SCC. Following issuance of this SSP, the GCC and SCC will collaborate to develop specific metrics for each of the remaining SSP activities identified in Section 4.3 that are designated for joint implementation. Finally, HPH stakeholders may choose to measure and report additional information on Sector progress during the National Annual Reporting process, as appropriate.

Table 3. Risk Assessment Priorities - Implementation Lead: RMWG. This table identifies priority metrics related to Sector risk assessment activities.

Priority	**Plan and execute a risk assessment methodology to assess the risks of physical, cyber, and human vulnerabilities and threats in the Sector.** (Implementation Lead: RMWG)	**Quarter**
Descriptive Data	Capture/report level of engagement (i.e., attendance, agencies represented, etc.) at risk assessment planning/development events.	
Output Data	Develop a project plan detailing project concept, milestones, timelines, and deliverables. Finalize and disseminate the final threat/hazard assessment module component to Sector partners. Finalize and disseminate the final HPH risk assessment methodology tool to Sector partners. Begin executing risk assessment methodology and collecting data.	**Q4 CY2015** **Q2 CY2016** **Q1 CY2017** **Q2-4 CY2017**
Outcome Data	Collect and assess stakeholder feedback on the risk assessment methodology development process and final product. Determine level of use and/or quantify Sector adoption and use of the risk assessment methodology. Collect and assess stakeholder feedback on the risk assessment execution process as well as overall utility of the risk assessment methodology as applied to stakeholder use. Collect and assess stakeholder feedback on security/resilience enhancements made as a result of the risk assessment methodology and share the resultant information appropriately.	

Table 4. Risk Management Priorities: Implementation Lead: A&I WG. This table identifies priority metrics for risk management activities as related to a long-term risk mitigation plan for the HPH Sector.

Priority	**Develop a long-term risk mitigation plan and set priorities based on a Sector risk assessment, leveraging existing products developed by partners, healthcare trend analyses, and needs of critical infrastructure owners and operators.** (Implementation Lead: A&I WG)	**Quarter**
Descriptive Data	Quantify/catalog the risk mitigation needs expressed by critical infrastructure owners and operators. Capture/report level of engagement (i.e., attendance, agencies represented, etc.) at long-term risk mitigation plan/priorities planning and development events.	
Output Data	Develop long-term risk mitigation plan, including priorities based on Sector risk assessment, within 12 months of adoption of new risk assessment methodology. Track implementation of priorities identified in Sector risk mitigation plan.	**Q1 CY2018** **Q2-4 CY2018**
Output Data	Collect and assess stakeholder feedback on the long-term risk mitigation plan development process and final product. Determine level of engagement of Sector stakeholders in mitigation plan priority activities. Collect and assess stakeholder feedback on security/resilience enhancements made as a result of implementing the long-term risk mitigation plan. Collect information regarding the number and type of public and/or private sector entities that develop and implement tailored risk mitigation plans based on the overarching Sector plan. Quantify/report on resolution of unmet priorities identified during the planning process.	

Table 5. Risk Management Priorities: Implementation Lead: Cybersecurity WG. This table identifies priority metrics for risk management activities as related to HPH Sector implementation of the NIST Cybersecurity Framework.

Priority	Develop guidance, in coordination with DHS, for Sector implementation of the NIST Cybersecurity Framework. (Implementation Lead: Cybersecurity WG)	Quarter
Descriptive Data	Collect/report NH-ISAC and HITRUST derived data (use profiles, information requests, web traffic and other cybersecurity stakeholder engagement information). Collect/report on GCC-SCC working group activities that focus on cyber threats and address cybersecurity.	
Output Data	Establish a joint GCC-SCC working group to focus on cyber threats and address cybersecurity. In conjunction with DHS, develop and issue NIST Cybersecurity Implementation Guidance and supporting tools. Develop collateral materials to encourage use of NIST Cybersecurity Framework. Leverage NH-ISAC and HITRUST to expand cybersecurity expert participation in the HPH Sector partnership. Generate materials and tools to address relevant HPH Sector privacy and cybersecurity issues.	**Q3 CY2015** **Q2 CY2016** **Q3 CY2016** **Q3 CY2016** **Q4 CY2016**
Outcome Data	Collect/assess stakeholder feedback on Sector guidance and supporting tools for implementing the NIST Cybersecurity Framework. Collect data/report number of SCC members who use NIST cybersecurity framework as well as related user feedback. Collect feedback on and track use of NIST Cybersecurity Framework-related materials generated by Sector partners. Quantitatively measure and report cybersecurity information sharing—including threat, response, mitigation, and remediation information—among Sector partners. Collect metrics on employment of NIST Cybersecurity Framework, with the goal of increasing the proportion of SCC members and number of Sector partners adopting the NIST Cybersecurity Framework.	

Table 6. Information Sharing Sector Priorities-Implementation Lead: A&I WG. This table identifies priority metrics for information sharing activities as related to assessing the effectiveness of Sector information sharing processes, systems, and mechanisms.

Priority	**Assess the effectiveness of current processes, mechanisms, and systems used to share information among Sector partners.** (Implementation Lead: A&I WG)	**Quarter**
Descriptive Data	Review all current HPH Sector information-sharing mechanisms and tools.	
Output Data	Compile, update, and publish "marketing" information on current Sector information-sharing mechanisms and tools: HSIN, public-facing websites, and text messaging programs. Collect data on existing Sector information-sharing processes, mechanisms, and systems. Develop recommendations about leveraging information-sharing systems based on the results of the assessment.	**Q1 CY 2016** **Q1 CY 2016** **Q2-3 CY 2016**
Outcome Data	Report on any information-sharing needs that are unmet by existing information processes, mechanisms, and systems. Reconfigure existing systems or add new systems or components to maximize information sharing capabilities. Collect/quantify information on Sector partner participation and expansion of such participation, access to and use of information-sharing tools and mechanisms, as well as feedback on the quality of those tools and mechanisms. Collect/quantify information on Sector partner participation in collaborative efforts such as Suspicious Activity Reporting and Fusion Centers, as well as feedback on the quality of those efforts.	

Table 7. Information Sharing Sector Priorities-Implementation Lead: Cybersecurity WG. This table identifies priority metrics for strengthening Sector two-way information sharing as related to cybersecurity incidents and gaps.

Priority	**Strengthen the dialogue between government and private sector partners about the challenges and benefits of two-way information sharing, particularly with respect to what can be shared, and cybersecurity incidents and gaps.** (Implementation Leads: Cybersecurity WG)	**Quarter**
Descriptive Data	Collect data regarding Sector partner cyber information-sharing needs and concerns. Collect and compile data on all cyber information-sharing mechanisms and tools in use within other critical infrastructure sectors.	
Output Data	Compile, update, and publish "marketing" information on current Sector cyber information-sharing mechanisms and tools. Develop and implement a strategy to educate Sector partners on the importance of and mechanisms for sharing PCII. Develop guidance on how cyber information (including threats, vulnerabilities, and mitigation measures) can be shared by the private sector and with the Federal Government. Update all documents based on partner feedback.	**Q2 CY2016** **Q3 CY2016** **Q4 CY2016** **Q1-4 CY2017**
Outcome Data	Collect/quantify information on Sector partner participation in collaborative partner efforts to enhance Sector cybersecurity, as well as feedback on the quality of those efforts. Collect Sector feedback on cyber information-sharing awareness, training, and education programs and activities.	

Table 8. Partnership Development and Coordination Priorities- Implementation Leads: SCC/GCC Leadership and A&I WG. This table identifies priority metrics for developing a HPH Partnership Engagement Strategy and supporting outreach materials.

Priority	**Develop a "Partnership Engagement Strategy" that enhances existing and develops new outreach material, and determines key partners that are not currently engaged in SCC/GCC activities.** (Implementation Leads: SCC/GCC Leadership and A&I WG)	**Quarter**
Descriptive Data	Collect and review existing marketing materials in use by the HPH Sector as well as other sectors. Analyze current partners within GCC/SCC and identify gaps in expertise and organizations.	
Output Data	Develop a partnership gap analysis. Develop and disseminate awareness and educational materials for the HPH Sector partnership with a focus on new members. Develop and implement a HPH Sector Partnership Engagement Strategy, including a comprehensive value proposition.	**Q1 CY2016** **Q2 CY2016** **Q3 CY2016**
Outcome Data	Engage partners in development of materials and garner Sector partner feedback following dissemination via surveys and other tools.	

Table 9. Partnership Development and Coordination Priorities- Implementation Leads: SCC/GCC Leadership and A&I WG. This table identifies priority metrics for analyzing and broadening partnerships to support HPH critical infrastructure security and resilience.

Priority	**Analyze and broaden partnerships to support critical infrastructure security and resilience and better understand the relationship between HPH critical infrastructure and community resilience.** (Implementation Leads: SCC/GCC Leadership and A&I WG)	**Quarter**
Descriptive Data	Conduct research on the makeup and representative nature of current Sector partnership members. Collect information relative to HPH Sector entities not yet formally part of the NIPP partnership framework, with a focus on private sector owners and operators. Collect information relative to the value proposition used to expand partnerships in other sectors. Collect information on community resilience activities relevant to critical infrastructure partnership.	
Output Data	Develop a candidate list of potential new Sector members. Engage additional cyber experts to join the partnership. Develop and disseminate awareness and educational materials on relevant community resilience activities.	**Q4 CY2015** **Q1 CY2016** **Q3 CY2016**
Outcome Data	Collect/report data regarding expansion of the GCC/SCC membership to fill gaps in representation (i.e., participation numbers in the GCC-SCC Joint Meeting) and on overall partnership value and effectiveness of specific partnership activities. Quantify/report on the increase in the number of GCC/SCC members with experience and expertise in cybersecurity.	

Table 10. Response and Recovery Priorities- Implementation Lead: SCC/GCC Leadership. This table identifies priority metrics for clarifying response and recovery roles and functions among HPH Sector partners.

Priority	**Clarify response and recovery roles and functions among FSLTT government, healthcare coalitions, and the private sector, including PPD-8 and ESF-8 activities.** (Implementation Lead: SCC/GCC Leadership)	Quarter
Descriptive Data	Gather descriptive data on HPH Sector engagement in PPD-8 related preparedness activities, including HPH infrastructure and cybersecurity gaps. Gather descriptive data on HPH Sector engagement during the response to and recovery from specific all-hazards disasters, including HPH infrastructure and cybersecurity gaps. Gather descriptive data on HPH Sector efforts to support continuity of operations planning for the Sector (involving lifeline sectors, communications, workforce planning, etc.).	
Outcome Data	Develop and make available PPD-8, NRF, and ESF-8 related awareness, education, and training materials for Sector partners, including webinars and web-based materials. Develop and deploy physical and cyber incident response checklists for Sector partners. Ensure resources for infrastructure planning, response, and recovery operations, such as clearances, HSIN access, Wireless Priority Service/GETS programs, and C3 Voluntary Program resources, are available to Sector partners.	**Q3-4 CY2016** **Q3-4 CY2016** **Q4 CY2016**
Output Data	Collect quantitative stakeholder feedback on access to and adequacy of resources for planning, response, and recovery activities. Collect/assess data regarding Sector partner participation in incident-related conference calls and solicit feedback on the efficacy of such calls. Solicit feedback on HPH Sector participation in real world incidents through the after-action and lessons-learned reporting processes.	

Table 11. Response and Recovery Priorities- Implementation Leads: RMWG; Cybersecurity WG. This table identifies priority metrics for the conduct of cybersecurity training and exercises and the cataloguing of resulting lessons learned among HPH Sector partners.

Priority	**Exercise the entire Sector partnership, both at the sector level and through national-level all-hazards exercises, including cyber, such as Cyber Storm V.** (Implementation Leads: RMWG; Cybersecurity WG)	**Quarter**
Descriptive Data	Collect/make available information on training and exercise activities relevant to the Sector (including Cyber Storm V) via the HHS CIP Office website. Disseminate information on the Homeland Security Exercise and Evaluation Program toolkit to Sector partners. Describe and report on lessons learned via Sector training and exercise activities.	
Outcome Data	Conduct training and exercise events with maximum participation from across the Sector. Develop and deploy an annual HPH Sector training and exercise plan and supporting schedule and support maximum participation from across the Sector. Develop and implement a process to capture and make available to Sector partners response, training, and exercise lessons learned.	**Q2 CY2016 – Q4 CY2017** **Q1 CY2017** **Q1 CY2017**
Output Data	Quantify/report number and type of Sector partners engaged in the planning and execution of Sector training and exercises (including Cyber Storm V). Collect Sector feedback on exercise participation through the after action reporting and improvement planning process (including Cyber Storm V). Collect Sector partner feedback regarding the incorporation of lessons learned into stakeholder risk mitigation plans, prevention plans, response plans, and/or related resources.	

7 Conclusion

The HPH Sector's critical infrastructure assets, systems, and professional workforce operate in a highly complex and dynamic risk environment. As discussed, this risk environment comprises a diverse and complicated mix of manmade and naturally occurring threats and hazards. From an operating perspective, HPH Sector infrastructure is vast and highly distributed, increasingly interdependent and interconnected, and inherently vulnerable due to the nature of its "open access" mission, physical facilities and operations, supply chains, and system interconnections. To understand and address existing and emergent risks given these complexities, HPH government and private sector partners must work together to develop and implement collaborative approaches tailored to the realities of the Sector's policy, operational, and risk environments.

The vision, goals, priorities, information sharing mechanisms, and partnership structures detailed in Sections 3, 4, and 5 of this SSP define the path forward in carrying out the HPH Sector mission across the various segments of the National Preparedness Framework established by PPD-8. Through implementation of this SSP over the next four years, the HPH Sector is also committed to fulfilling its responsibilities under PPD-21, E.O. 13636, the NIPP 2013, and the NHSS to secure and enhance the resilience of HPH critical infrastructure across its human, physical, and cyber dimensions. To do so, the Sector will leverage diverse authorities, capabilities, expertise, and resources collaboratively across all levels of the vast HPH partnership network, buttressed by dynamic, all-hazards information sharing among Sector partners. Through the initial performance metrics established in Section 6—together with those to be subsequently developed by HPH SCC and GCC partners following issuance of this SSP—the Sector leadership will track and measure progress against the achievement of Sector goals and priorities and receive important feedback relative to the collective reduction of identified risks to Sector infrastructure assets and people.

The continuously evolving nature of the threat environment in which the Sector operates requires an equally dynamic approach to risk management. Hence, the HPH Sector goals, priority activities, performance metrics, and partnership and information sharing mechanisms identified in this SSP are intended to be flexible in their application. They also are intended to accommodate modifications, updates, and reprioritization as necessary to keep pace with evolving threats, hazards, vulnerabilities, and corresponding changes in the national and sector policy environments. The Sector's vision—*a public-private partnership supporting the needs of HPH critical infrastructure and FSLTT government partners to enhance the resilience of the Sector to all hazards*—and mission—*to sustain the essential functions of the Nation's healthcare and public health delivery system and to support effective emergency preparedness and response to nationally significant hazards*—remain constant throughout.

8 Appendices

Appendix A: HPH Sector Priorities Mapped to NIPP 2013 National Call to Action

Appendix B: HPH Priorities Mapped to Joint National Priorities and NIPP 2013 Goals

Appendix C: NIST Cybersecurity Framework Goals and HPH Sector Cybersecurity Activities Crosswalk

Appendix D: ASPR Programs and Activities Relevant to Critical Infrastructure Security and Resilience

Appendix E: Authorities

Appendix F: Acronyms

Appendix G: Key Definitions

Appendix H: Additional References

Appendix A: Healthcare and Public Health Sector Priorities Mapped to the National Call to Action

Table A-1. This table maps the HPH Sector priorities to the NIPP National Call to Action. The National Call to Action items are located in the far left column and the Sector's priorities are listed in the top row. "X's" show commonality between the two.

National call to action items	Risk assessment methodology	Risk mitigation plan and priorities	Implementation of NIST Cybersecurity Framework	Assessment of information-sharing methods	Strengthen the dialogue	Partnership Engagement Strategy	Analyze and broaden partnerships	Clarify response and recovery roles and functions	Exercise Sector partnership
1. Set national focus through jointly developed priorities.		X	X	X	X	X	X		
2. Determine collective actions through joint planning efforts.	X	X	X						
3. Empower local and regional partnerships to build capacity nationally.	X	X	X	X	X	X	X	X	X
4. Leverage incentives to advance security and resilience.		X	X	X	X		X		
5. Enable risk-informed decision-making through enhanced situational awareness.	X	X		X	X		X	X	

National call to action items	Risk assessment methodology	Risk mitigation plan and priorities	Implementation of NIST Cybersecurity Framework	Assessment of information-sharing methods	Strengthen the dialogue	Partnership Engagement Strategy	Analyze and broaden partnerships	Clarify response and recovery roles and functions	Exercise Sector partnership
6. Analyze infrastructure dependencies, interdependencies, and associated cascading effects during and following incidents.	X	X					X	X	
7. Identify, assess, and respond to unanticipated infrastructure cascading affects during and following incidents.	X	X						X	
8. Promote infrastructure, community, and regional recovery following incidents.	X	X			X		X	X	
9. Strengthen coordinated development and delivery of technical assistance, training, and education.			X		X				X

National call to action items	Risk assessment methodology	Risk mitigation plan and priorities	Implementation of NIST Cybersecurity Framework	Assessment of information-sharing methods	Strengthen the dialogue	Partnership Engagement Strategy	Analyze and broaden partnerships	Clarify response and recovery roles and functions	Exercise Sector partnership
10. Improve critical infrastructure security and resilience by advancing R&D solutions.		X					X		
11. Evaluate progress toward the achievement of goals.		X	X		X				
12. Learn and adapt during and after exercises and incidents.		X						X	X

Appendix B: Healthcare and Public Health Priorities Mapped to the Joint National Priorities (JNPs) and National Infrastructure Protection Plan 2013 Goals

Table B-1. This table shows the alignment of the HPH Sector Priorities, NIPP 2013 priorities, and the JNPs.

Healthcare and Public Health Sector Priorities	**JNP: Strengthen Management of Cyber and Physical Risks to Critical Infrastructure**	**JNP: Build Capabilities and Coordination for Enhanced Incident Response and Recovery**	**JNP: Strengthen Collaboration Across Sectors, Jurisdictions and Disciplines**	**JNP: Enhance Effectiveness in Resilience Decision-Making**	**JNP: Share Information to Improve Prevention, Mitigation, Response, and Recovery Activities**	**NIPP Goals**
Plan and execute a risk assessment methodology to assess the risks of physical, cyber and human vulnerabilities and threats in the Sector.	X			X	X	Assess and analyze risks to critical infrastructure (including threats, vulnerabilities, and consequences) to inform risk management activities.
Develop a long-term risk mitigation plan and set priorities based on a Sector risk assessment, leveraging existing products developed by partners, healthcare trend analyses, and needs of critical infrastructure owners and operators.	X		X	X	X	Secure critical infrastructure against physical, cyber, and human threats through sustainable risk reduction efforts, while considering costs and benefits.
Develop guidance, in coordination with DHS, for Sector implementation of the NIST Cybersecurity Framework.	X				X	Secure critical infrastructure against physical, cyber, and human threats through sustainable risk reduction efforts, while considering costs and benefits.

Healthcare and Public Health Sector Priorities	JNP: Strengthen Management of Cyber and Physical Risks to Critical Infrastructure	JNP: Build Capabilities and Coordination for Enhanced Incident Response and Recovery	JNP: Strengthen Collaboration Across Sectors, Jurisdictions and Disciplines	JNP: Enhance Effectiveness in Resilience Decision-Making	JNP: Share Information to Improve Prevention, Mitigation, Response, and Recovery Activities	NIPP Goals
Assess the effectiveness of current processes, mechanisms, and systems used to share information among Sector partners.		X	X	X	X	
Strengthen the dialogue between government and private sector partners about the challenges and benefits of two-way information sharing, particularly with respect to what can be shared, and cybersecurity incidents and gaps.	X		X		X	Enhance critical infrastructure resilience by minimizing consequences and employing effective response and recovery.
Develop a "Partnership Engagement Strategy" that enhances existing and develops new outreach material, and determines key partners that are not currently engaged in SCC/GCC activities.	X		X		X	Share information across the critical infrastructure community to build awareness and enable risk-informed decision-making.
Analyze and broaden partnerships to support critical infrastructure security and resilience and to better understand the relationship between HPH critical infrastructure and community resilience.			X	X		Share information across the critical infrastructure community to build awareness and enable risk-informed decision-making.

Healthcare and Public Health Sector Priorities	JNP: Strengthen Management of Cyber and Physical Risks to Critical Infrastructure	JNP: Build Capabilities and Coordination for Enhanced Incident Response and Recovery	JNP: Strengthen Collaboration Across Sectors, Jurisdictions and Disciplines	JNP: Enhance Effectiveness in Resilience Decision-Making	JNP: Share Information to Improve Prevention, Mitigation, Response, and Recovery Activities	NIPP Goals
Clarify response and recovery roles and functions among FSLTT government, healthcare coalitions, and the private sector, including PPD-8 and ESF-8 activities.		X		X		Share information across the critical infrastructure community to build awareness and enable risk-informed decision-making.
Exercise the entire Sector partnership, both at the Sector level and through national-level, all-hazards exercises, including cyber, such as Cyber Storm V.		X	X	X		Promote learning and adaptation during and after incidents and exercises.

Appendix C: National Institute of Standards and Technology Cybersecurity Framework Goals and Healthcare and Public Health Sector Cybersecurity Activities Crosswalk

Table C-1. This table shows the alignment of HPH Sector cybersecurity activities with the goals established in the NIST Cybersecurity Framework.

HPH Sector Cybersecurity Activities	**NIST Goal: Critical systems and functions are identified and prioritized, and cyber risk is understood as part of a risk management plan.**	**NIST Goal: Risk-informed actions are taken to protect critical systems and functions.**	**NIST Goal: Resources are coordinated and applied to triage and respond to cyber events and incidents in order to minimize impacts to critical systems and functions.**	**NIST Goal: Following a cyber incident, impacted critical systems and functions are reconstituted based on prior planning and informed by situational awareness.**	**NIST Goal: Adverse cyber activities are detected, and situational awareness of threats is maintained.**	**NIST Goal: Security and resilience are continually improved based on lessons learned, consistent with risk management planning.**
Efforts in collaboration with the DHS Office of Cybersecurity and Communications to support the C³ Voluntary Program, which serves as the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes. The program supports Sector partners in increasing cyber resilience and the Sector's awareness and use of the NIST Framework for Improving Critical Infrastructure Cybersecurity.	X	X			X	X

HPH Sector Cybersecurity Activities	NIST Goal: Critical systems and functions are identified and prioritized, and cyber risk is understood as part of a risk management plan.	NIST Goal: Risk-informed actions are taken to protect critical systems and functions.	NIST Goal: Resources are coordinated and applied to triage and respond to cyber events and incidents in order to minimize impacts to critical systems and functions.	NIST Goal: Following a cyber incident, impacted critical systems and functions are reconstituted based on prior planning and informed by situational awareness.	NIST Goal: Adverse cyber activities are detected, and situational awareness of threats is maintained.	NIST Goal: Security and resilience are continually improved based on lessons learned, consistent with risk management planning.
Identification and ongoing review of HPH Sector critical cybersecurity functions and services as part of the Cyber-Dependent Infrastructure Identification effort mandated in Executive Order 13636. This effort identified Sector critical functions that were validated by Sector subject matter experts.	X					X
Incorporation of cybersecurity considerations as part of the Sector risk assessment methodology effort described in Section 5.1.3 to help inform sector-specific risk management strategies and decision-making and to provide a linkage between national and organizational cyber risk management efforts.	X	X		X		X

HPH Sector Cybersecurity Activities	NIST Goal: Critical systems and functions are identified and prioritized, and cyber risk is understood as part of a risk management plan.	NIST Goal: Risk-informed actions are taken to protect critical systems and functions.	NIST Goal: Resources are coordinated and applied to triage and respond to cyber events and incidents in order to minimize impacts to critical systems and functions.	NIST Goal: Following a cyber incident, impacted critical systems and functions are reconstituted based on prior planning and informed by situational awareness.	NIST Goal: Adverse cyber activities are detected, and situational awareness of threats is maintained.	NIST Goal: Security and resilience are continually improved based on lessons learned, consistent with risk management planning.
Establishment of a joint GCC-SCC working group to focus on cyber threats and address cybersecurity. The working group will consider cyber risks, such as loss of system availability, data integrity, confidentiality, and privacy. It will also identify consequences and cascading effects, as well as mitigation strategies.	X	X	X	X		X
Expansion of cybersecurity expert participation in the HPH Sector partnership and expanded focus on cybersecurity information sharing—including threat, response, mitigation, and remediation information—among Sector partners through the services provided by the NH-ISAC and HITRUST.	X	X	X	X	X	X
Development of guidance for Sector implementation of the NIST Cybersecurity Framework.	X	X	X	X	X	X

HPH Sector Cybersecurity Activities	**NIST Goal: Critical systems and functions are identified and prioritized, and cyber risk is understood as part of a risk management plan.**	**NIST Goal: Risk-informed actions are taken to protect critical systems and functions.**	**NIST Goal: Resources are coordinated and applied to triage and respond to cyber events and incidents in order to minimize impacts to critical systems and functions.**	**NIST Goal: Following a cyber incident, impacted critical systems and functions are reconstituted based on prior planning and informed by situational awareness.**	**NIST Goal: Adverse cyber activities are detected, and situational awareness of threats is maintained.**	**NIST Goal: Security and resilience are continually improved based on lessons learned, consistent with risk management planning.**
Coordination with the NH-ISAC and HITRUST to assist in the implementation of Executive Order 13691, Improving Private Sector Information Sharing.	X	X	X		X	X
Encouragement and coordination of Sector participation in planning and conducting the Cyber Storm series of exercises.						X
Develop a cyber concept of operations to explain the actions taken if a private sector entity reports a breach or cyberattack.			X	X	X	

Appendix D: Office of the Assistant Secretary for Preparedness and Response Programs and Activities Relevant to Critical Infrastructure Security and Resilience

ASPR Program/Activity	Role in Critical Infrastructure Security and Resilience
Biomedical Advanced Research and Development Authority	Funds advanced R&D for manufacturing, tasking, stockpiling, and acquiring medical countermeasures (MCMs) for preparedness and response. Coordinates security and resilience of partnered facilities producing needed MCMs, including vaccines, therapeutics, diagnostics, and non-pharmaceutical countermeasures, against manmade and emerging infectious disease threats, such as pandemic influenza and Ebola. Ensures that MCM manufacturing facilities are considered as part of the Nation's critical infrastructure and are included on priority infrastructure lists. Ensures such facilities are able to continue operations in the face of disasters.
Continuity of Operations	The ASPR Office of Emergency Management (OEM) leads efforts to plan for and exercise the continuity of operations of HPH functions. OEM incorporates post-incident health recovery through the Health and Social Services Recovery Support Functions (RSF) concept of operations. It also builds relationships with strategic partners to leverage opportunities and advance the Sector's recovery mission and supporting operations.
Healthcare Preparedness Program	Provides grant funding and guidance to recipients to support the development and improvement of hospital preparedness activities. Healthcare Preparedness Program awardees are encouraged to adopt practices that ensure their healthcare facilities can retain operational capacity throughout disasters or have the ability to quickly return to operational capacity after an event.
Policy and Strategic Planning	ASPR's policy and planning responsibilities include coordinating and leading development of national strategies and policies by participating in departmental strategic planning and evaluation efforts and by promoting preparedness, response, and recovery policy development and analysis across ASPR and HHS, federally, nationally, and internationally. ASPR champions efforts to improve policy and planning frameworks to most effectively and efficiently allow for progress and improvement rooted in the evidence base for preparedness, response, and recovery. ASPR also develops and coordinates implementation of the NHSS and leads the coordination of HHS responsibilities under PPD-21, E.O. 13636, and the NIPP 2013, among other national preparedness plans.
Response and Recovery	Facilitates and coordinates response and recovery activities with SLTT governments and the private sector. As the primary agency for ESF 8, Public Health and Medical Services, the HHS Secretary has designated ASPR to direct and coordinate all Federal public health and medical assistance provided under ESF-8. ASPR acts as the senior-level HHS liaison to DHS and other Federal departments and agencies during ESF-8 response.
Regional Emergency Coordinators	Provide health and medical support according to FEMA designated regions. Coordinates with State and local governments to enhance preparedness and response.

Appendix E: Acronyms

A&I WG	Awareness and Implementation Working Group
ASPR	Assistant Secretary for Preparedness and Response
C3	Cyber Threat Intelligence and Incident Coordination Center
CDC	Centers for Disease Control
CIP	ASPR Critical Infrastructure Protection Program Office
CIPAC	Critical Infrastructure Partnership Advisory Council
CONOPS	Concept of Operations Plan
CS&C	DHS Office of Cybersecurity and Communications
CSCSWG	Cross-Sector Cyber Security Working Group
Cyber UCG	Cyber Unified Coordination Group
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
E.O.	Executive Order
EMP	Electromagnetic Pulse
ESF	Emergency Support Function
ESS	Emergency Services Sector
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
FSLTT	Federal, State, local, tribal, and territorial
GCC	Government Coordinating Council
GETS	Government Emergency Telecommunications Service
Health IT	Health Information Technology
HHS	U.S. Department of Health and Human Services
HITRUST	Health Information Trust Alliance
HSA	Homeland Security Advisor
HSIN	Homeland Security Information Network
HPH	Healthcare and Public Health

I&A	DHS Office of Intelligence and Analysis
ICS	Incident Command System
IP	DHS Office of Infrastructure Protection
ISAO	Information Sharing and Analysis Organizations
JNP	Joint National Priorities
MCM	Medical Countermeasures
MERS	Middle East Respiratory Syndrome
NCI	National Council of ISACs
NCCIC	National Cybersecurity and Communications Integration Center
NCIPP	National Critical Infrastructure Prioritization Program
NH-ISAC	Healthcare and Public Health Information Sharing and Analysis Center
NICC	National Infrastructure Coordinating Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NIST	National Institute for Standards and Technology
NHSS	National Health Security Strategy
NPPD	National Protection and Programs Directorate
NPG	National Preparedness Goal
NSI	Nationwide Suspicious Activity Reporting Initiative
OCIA	Office of Cyber and Infrastructure Analysis
ODNI	Office of the Director of National Intelligence
OEM	Office of Emergency Management
OHA	DHS Office of Health Affairs
ONC	Office of the National Coordinator for Health Information Technology
PCII	Protected Critical Infrastructure Information
PPD	Presidential Policy Directive
R&D	Research and Development
RMWG	Risk Management Work Group
RSF	Recovery Support Function

S&T	DHS Science and Technology Directorate
SARS	Severe Acute Respiratory Syndrome
SAR	Suspicious Activity Reporting
SCC	Sector Coordinating Council
SSA	Sector-Specific Agency
SLTT	State, Local, Tribal, and Territorial
SSP	Sector-Specific Plan
TRACIE	Technical Resources, Assistance Center, and Information Exchange
VA	Department of Veterans Affairs
WG	Workgroup

Appendix F: Authorities

DHS FEMA, Effective Coordination of Recovery Resources for State, Tribal, Territorial and Local Incidents, February 2015

HHS ASPR, National Health Security Strategy (NHSS) and Implementation Plan, 2014

National Protection Framework, July 2014

National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework), February 2014

DHS, National Infrastructure Protection Plan (NIPP) 2013, Partnering for Critical Infrastructure Security and Resilience, 2013

DHS FEMA, National Mitigation Framework 2013

DHS FEMA, National Response Framework, 2nd Edition, May 2013

DHS FEMA, National Prevention Framework, May 2013

Presidential Policy Directive / PPD-21: Critical Infrastructure Security and Resilience, February 2013

Executive Order (E.O.) 13636- Improving Critical Infrastructure Cybersecurity, February 2013 (Federal Register Vol. 78, No. 33)

Emergency Support Function #8, Health and Medical Services Annex, January 2013

DHS FEMA, National Disaster Recovery Framework, Strengthening Disaster Recovery for the Nation, September 2011

Presidential Policy Directive / PPD-8: National Preparedness, March 2011

DoD 6200.03 "Public Health Emergency Management within the Department of Defense" (January 14, 2010)

Homeland Security Presidential Directive (HSPD)-21: Public Health and Medical Preparedness, October 2007

Pandemic and All-Hazards Preparedness Act of 2006 (Public Law 109-417)

DHS Procedures for Handling Critical Infrastructure Information, Final Rule, 6 CFR Part 29 (September 1, 2006)

Project BioShield Act of 2004 (Public Law 108-276)

Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458)

HSPD-10: Biodefense for the 21st Century, April 2004

Veterans Affairs Department and Department of Defense Health Resources Sharing and Emergency Operations Act of 2002 (Public Law 97-174)

Homeland Security Information Sharing Act (Public Law 107-296), enacted as part of the Homeland Security Act of 2002

Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act)

Cybersecurity Enhancement Act of 2002 (Title II, Section 225, of the Homeland Security Act of 2002)

Title VIII, Section 817, of the USA Patriot Act of 2001 (Public Law 107-56)

Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (Public Law 107-188)

Department of Veteran Affairs Emergency Preparedness Act of 2002 (Public Law 107-287)

Public Health Threats and Emergencies Act of 2000 (Title I of the Public Health Improvement Act (Public Law 106-505))

Public Health Service Act of 1944 (42 United States Code (U.S.C.) 201-300hh-11)

HHS Continuity of Operations Plan (COOP) for Public Health and Medical Emergencies

Joint Commission "Hospital Incident Command System Guidebook," 5th Edition

Appendix G: Key Definitions

Many of the definitions below are derived from language enacted in Federal laws and/or included in national policies and/or plans, including the Homeland Security Act of 2002; the USA PATRIOT Act of 2001; the 2009 and 2013 NIPP; PPD-8, *National Preparedness*; and PPD-21, *Critical Infrastructure Security and Resilience,* among various others. Additional definitions come from the DHS Risk Lexicon. The source for each entry below follows each definition provided.

All Hazards. The term "all hazards" means a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure. (Source: PPD-21, 2013)

Asset. Person, structure, facility, information, material, or process that has value. (Source: DHS Risk Lexicon, 2010)

Business Continuity. Activities performed by an organization to ensure that during and after a disaster the organization's essential functions are maintained uninterrupted, or are resumed with minimal disruption. (Source: NIPP, 2013)

Consequence. The effect of an event, incident, or occurrence, including the number of deaths, injuries, and other human health impacts along with economic impacts both direct and indirect and other negative outcomes to society. (Source: Adapted from DHS Risk Lexicon, 2010)

Critical Infrastructure. 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. (Source: §1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e))

Critical Infrastructure Community. Critical infrastructure owners and operators, both public and private; Federal departments and agencies; regional entities; SLTT governments; and other organizations from the private and nonprofit sectors with a role in securing and strengthening the resilience of the Nation's critical infrastructure and/or promoting practices and ideas for doing so. (Source: NIPP, 2013)

Critical Infrastructure Cross-Sector Council. Private sector council that comprises the chairs and vice chairs of the SCCs. This council coordinates cross-sector issues and initiatives to support critical infrastructure security and resilience. (Source: NIPP, 2013)

Critical Infrastructure Information (CII). Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems. CII consists of records and information concerning any of the following:

- Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law; harms the interstate commerce of the United States; or threatens public health or safety. (Source: CII Act of 2002, 6 U.S.C. § 131)

• The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk management planning, or risk audit. (Source: CII Act of 2002, 6 U.S.C. § 131)

• Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, insurance, or continuity, to the extent that it is related to such interference, compromise, or incapacitation. (Source: CII Act of 2002, 6 U.S.C. § 131)

Critical Infrastructure Owners and Operators. Those entities responsible for day-to-day operation and investment of a particular critical infrastructure entity. (Source: NIPP, 2013)

Critical Infrastructure Partner. Those Federal and SLTT governmental entities, public and private sector owners and operators and representative organizations, regional organizations and coalitions, academic and professional entities, and certain not-for-profit and private volunteer organizations that share responsibility for securing and strengthening the resilience of the Nation's critical infrastructure. (Source: NIPP, 2013)

Critical Infrastructure Risk Management Framework. A planning and decision-making framework that outlines the process for setting goals and objectives, identifying infrastructure, assessing risks, implementing risk management activities, and measuring effectiveness to inform continuous improvement in critical infrastructure security and resilience. (Source: NIPP, 2013)

Cybersecurity. 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; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (Source: NIPP, 2013)

Dependency. The uni-directional reliance of an asset, system, network, or collection thereof—within or across sectors—on an input, interaction, or other requirement from other sources in order to function properly. (Source: NIPP, 2013)

Executive Order 13636. Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity framework; and promote and incentivize the adoption of strong cybersecurity practices. (Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013)

Emergency Support Functions (ESF). The primary, but not exclusive, Federal coordinating structures for building, sustaining, and delivering the response core capabilities. ESFs are vital for responding to Stafford Act incidents but also may be used for other incidents. (Source: National Response Framework, 2013)

Federal Departments and Agencies. Any authority of the United States that is an "agency" under 44 U.S.C. §3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. §3502(5). (Source: PPD-21, 2013)

Function. Service, process, capability, or operation performed by an asset, system, network, or organization. (Source: DHS Risk Lexicon, 2010)

Fusion Center. A State and major urban area focal point for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government, SLTT, and private sector partners. (Source: Adapted from the DHS Risk Lexicon, 2010)

Government Coordinating Council (GCC). The government counterpart to the Sector Coordinating Council for each sector, established to enable interagency and intergovernmental coordination; comprises representatives across various levels of government (Federal and SLTT) as appropriate to the risk and operational landscape of each sector. (Source: NIPP, 2013)

Hazard. Natural or manmade source or cause of harm or difficulty. (Source: DHS Risk Lexicon, 2010)

Healthcare Coalition. A healthcare coalition is a group of healthcare organizations, public safety and public health partners that join forces for the common cause of making their communities safer, healthier, and more resilient. (Source: National Healthcare Coalition Resource Center)

Incident. An occurrence, caused by either human action or natural phenomenon, that may cause harm and require action, which can include major disasters, emergencies, terrorist attacks, terrorist threats, wild and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, cyber-attacks, cyber failure/accident, and other occurrences requiring an emergency response. (Source: DHS Risk Lexicon, 2010)

Information Sharing and Analysis Centers (ISACs). Operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders. (Source: NIPP 2013)

Information Sharing and Analysis Organization. Any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of: (a) Gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof; (b) Communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or an incapacitation problem related to critical infrastructure or protected systems; and (c) Voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (a) and (b). (Source: Homeland Security Act of 2002, 6 U.S.C. § 131)

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; consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (Source: DHS Risk Lexicon, 2010)

Interdependency. Mutually reliant relationship between entities (objects, individuals, or groups); the degree of interdependency does not need to be equal in both directions. (Source: DHS Risk Lexicon, 2010)

Mitigation. Capabilities necessary to reduce loss of life and property by lessening the impact of disasters. (Source: PPD-8, 2011)

National Preparedness. The actions taken to plan, organize, equip, train, and exercise to build and sustain the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the security of the Nation. (Source: PPD-8, 2011)

Network. A group of components that share information or interact with each other to perform a function. (Source: NIPP, 2013)

Partnership. Close cooperation between parties having common interests in achieving a shared vision. (Source: NIPP, 2013)

Prevention. Those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. (Source: PPD-8, 2011)

Protected Critical Infrastructure Information (PCII). All critical infrastructure information that has been properly submitted and validated pursuant to the Critical Infrastructure Information Act and implementing directive; all information submitted to the PCII Program Office or designee with an express statement is presumed to be PCII until the PCII Program Office determines otherwise. (Source: CII Act of 2002, 6 U.S.C. § 131)

Protection. Those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. (Source: PPD-8, 2011)

Recovery. Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources. (Source: PPD-8, 2011)

Recovery Support Functions (RSF). Coordinating structures for key functional areas of assistance during recovery operations; RSFs support local governments by facilitating problem solving, improving access to resources, and fostering coordination among State and Federal agencies, nongovernmental partners, and stakeholders. (Source: National Disaster Recovery Framework, 2011)

Regional. Entities and interests spanning geographic areas ranging from large multi-State areas to metropolitan areas and varying by organizational structure and key initiatives, yet fostering engagement and collaboration between critical infrastructure owners and operators, government, and other key

stakeholders within the given location. (Source: Regional Partnerships: Enabling Regional Critical Infrastructure Resilience, RC3, March 2011)

Response. Capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. (Source: PPD-8, 2011)

Risk. The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. (Source: DHS Risk Lexicon, 2010)

Risk-Informed Decision-Making. The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other relevant factors. (Source: NIPP, 2013)

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; the National Plan addresses 16 critical infrastructure sectors, as identified in PPD-21. (Source: NIPP, 2013)

Sector Coordinating Council (SCC). The private sector counterpart to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector. They serve as principal entry points for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. (Source: NIPP, 2013)

Sector-Specific Agency (SSA). A Federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (Source: PPD-21, 2013)

Sector-Specific Plans (SSP). Planning documents, developed by the SSAs in close collaboration with the SCCs and other sector partners, that complement and tailor application of the National Plan to the specific characteristics and risk landscape of each critical infrastructure sector. (Source: NIPP, 2013)

Secure/Security. Reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters. (Source: PPD-21, 2013)

Stakeholder. The NIPP does not define the word “stakeholder;” but to understand the distinction between partners and stakeholders, it is useful to refer to the definitions of Critical Infrastructure Partners and Critical Infrastructure Community above. Partners share responsibility for strengthening critical infrastructure security and resilience, while stakeholders may play a role in strengthening critical infrastructure security and resilience and/or promoting practices and ideas for doing so. In addition, stakeholders may simply have an interest in critical infrastructure security and resilience based on their involvement in related disciplines or activities. For example, Congress, the White House, and the Government Accountability Office are all critical infrastructure stakeholders.

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. (Source: DHS Risk Lexicon, 2010)

System. Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose. (Source: DHS Risk Lexicon, 2010)

Terrorism. Premeditated threat or act of violence against noncombatant persons, property, and environmental or economic targets to induce fear, intimidate, coerce, or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives. (Source: DHS Risk Lexicon, 2010)

Threat. A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. (Source: DHS Risk Lexicon, 2010)

Threat and Hazard Identification and Risk Assessment (THIRA). A tool that allows a regional, State, or urban area jurisdiction to understand its threats and hazards and how the impacts may vary according to time of occurrence, season, location, and other community factors. This knowledge helps a jurisdiction establish informed and defensible capability targets for preparedness. (Source: FEMA web site)

Value Proposition. A statement that outlines the business and national interest in critical infrastructure security and resilience actions and articulates the benefits gained by partners through collaborating in the mechanisms described in the National Plan. (Source: NIPP, 2013)

Vulnerability. A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. (Source: DHS Risk Lexicon, 2010)

Appendix H: Additional References

HHS, Incorporating Active Shooter Incident Planning Into Health Care Facility Emergency Operations Plans, November 2014.

Healthcare and Public Health Sector Coordinating Council, Active Shooter Planning and Response in a Healthcare Setting, April 2015.

The Joint Commission Sentinel Event Alert, Preventing Violence in the Health Care Setting, Issue 45, June 3, 2010.