Chemical Sector-Specific Plan

An Annex to the NIPP 2013

2015

Homeland Security

TABLE OF CONTENTS

COORDINATION LETTER FROM COUNCIL CHAIRS

In 2003, the Federal Government designated the Chemical Sector as a critical infrastructure sector, recognizing its significant contribution to national security and the economy. Since then, the sector has successfully built public-private partnerships, which improved information sharing, created forums to share best practices, and developed tools and exercises to improve incident response and recovery. The sector recognizes the value of partnership and continues to take steps to improve security and resilience.

2015 Sector-Specific Plan Update

This 2015 release of the Chemical Sector-Specific Plan (SSP) updates the original plan issued in May 2007 and the update of 2010. As with the previous plans, this SSP represents a collaborative effort among the private sector; Federal, State, local, tribal, and territorial governments; and nongovernmental organizations to reduce critical infrastructure risk.

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

Key Accomplishments

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

- Co-hosted the annual Chemical Sector Security Summit, which provides a forum for nearly 500 members of the Chemical Sector community to exchange security-related information, share best practices, and gain insight into the roles of government partners that support chemical security and resilience efforts.
- Developed the *Playbook for an Effective All-Hazards Chemical Sector Response*, which outlines private and public sector roles and responsibilities in preparing for, responding to, and recovering from all-hazards emergencies. The updated Playbook was exercised during an incident information-sharing tabletop exercise at the 2014 Chemical Sector Security Summit.
- Transferred experimental results from Project Jack Rabbit on the toxic inhalation hazards of chlorine and ammonia to train Hazardous Material (HAZMAT) operators and first responders in local communities and at chemical facilities. The project also received regional and national awards for excellence in technology transfer in 2013 and 2014 from the Federal Laboratory Consortium. The sector also initiated Jack Rabbit II, which will seek to incorporate source terms gathered from catastrophic dense gas releases into dispersion modeling and simulation tools.
- Certified 21,689 of 24,895 individuals who registered to take the Web-based Chemical Security Awareness Training program since July 2008.
- Developed a cross-sector Web-based course, "Theft and Diversion – What You Can Do," to provide owners and operators with the information needed to identify and take action to prevent the theft and diversion of resources, raw materials, technologies, and products. Since its launch in February 2013, the course has been completed by a total of 5,405 individuals, 3,603 of whom were from the private sector.
- Developed and delivered classified briefings detailing current threats to industrial control systems (ICS) with the U.S. Department of Homeland Security (DHS) and in partnership with other Federal agencies and government partners.

- Distributed 18,000 security resources—through the Chemical Sector-Specific Agency (SSA)—such as awareness guides and DVDs that promote common security activities. DHS continues to work with industry partners to address gaps and develop resources to strengthen infrastructure security.
- Actively engaged in discussions regarding Executive Order 13650: Improving Chemical Facility Safety and Security (EO 13650), which shaped the Federal Government's report to the President entitled *Actions to Improve Chemical Facility Safety and Security – A Shared Commitment*. The report incorporates input from nearly 1,800 stakeholders that participated in listening sessions and Webinars and provides the Federal Government's action plan for continued improvement in chemical safety and security and further reduction in risks to workers, communities, and first responders.

These achievements represent the effective and value-added collaboration among the Chemical SCC, GCC, and DHS as the Chemical SSA. They clearly demonstrate the sector's progress and collaborative approach to developing, prioritizing, and implementing effective security programs and resilience strategies.

In the same shared purpose that guided these actions and their support for the framework, concepts, and processes outlined in the NIPP 2013, Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21), EO 13650, and Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636), Chemical Sector partners will continue their efforts to enhance the security and resilience of the Nation's critical infrastructure assets.

Rollie Shook

Rollie B. Shook
Chair
Chemical Sector
Coordinating Council

Caitlin A. Durkovich
Assistant Secretary
Office of Infrastructure Protection
U.S. Department of Homeland Security
Chair, Chemical Sector Government Coordinating Council

EXECUTIVE SUMMARY

The Chemical Sector converts raw materials into more than 70,000 diverse products and is a major component of the U.S. economy, contributing approximately 25 percent of the Nation's gross domestic product (GDP).[*] The Chemical Sector employs nearly 800,000 workers who manufacture, store, and transport chemicals to customers in multiple critical infrastructure sectors. About 96 percent of U.S. goods in 2013 were manufactured using Chemical Sector products, making uninterrupted chemical production and transportation essential for national and economic security.

Chemical Sector Assets and Risks

The majority of chemical manufacturing, transportation, storage, and warehousing facilities are privately owned and operated. Because of their potential health and safety hazards, chemicals must be carefully managed from manufacturing to end use in research, pharmaceutical, agricultural, petrochemical, and water treatment applications, to name a few. With facilities, suppliers, and end users located around the globe, Chemical Sector operations are vulnerable to a variety of disruptions stemming from natural disasters, extreme weather, cyberattacks, biohazards, and pandemics. Local or regional disruptions to critical suppliers can cause cascading disruptions across geographic regions and in multiple industries.

Owners and operators should secure their products from theft and diversion for use in chemical or explosive weapons. The Chemical Sector now faces increasingly sophisticated cyber adversaries and a growing concern among operators of insider threats. Owners and operators also find it difficult to accurately characterize the likelihood of known threats to a specific facility, making it difficult to prioritize security measures.

Partnering to Improve Security and Resilience

Owners and operators in the Chemical Sector assess their facility risks and establish security, business continuity, and emergency response plans to mitigate individual risks. The highest-risk Chemical Sector facilities are regulated for security through multiple Federal agencies. Outside of regulations, Chemical Sector owners and operators have a strong history of working in partnership to develop industry practices that build a culture of safety and security.

The *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013) partnership structure encourages owners and operators to work directly with their peers through the Chemical Sector Coordinating Council (SCC). It also enables the SCC to work closely with government counterparts at all levels through the Chemical Government Coordinating Council (GCC). Partners work on a voluntary basis to share actionable, relevant risk information; exchange best practices; build cross-sector situational awareness; and enable risk-informed decision-making.

Through this partnership, the Chemical Sector has developed tools, resources, and programs that support sector-wide risk management and maximize partners' limited resources. Key examples include tabletop exercises and training workshops focused on effective communication during security incidents, business continuity best practices, an annual Chemical Sector Security Summit, classified threat briefings for cleared owners and operators, and the Chemical Security Awareness Training Program.

2015 Sector-Specific Plan

This Chemical Sector-Specific Plan (SSP) is designed to guide the sector's collaborative efforts to improve security and resilience during the next four years. It describes how the Chemical Sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21). As an annex to the NIPP 2013, this SSP tailors national strategic guidance to the unique operating conditions and risk landscape of the Chemical Sector. As such, the sector strategy supports the NIPP 2013 national goals and strategy, the 2014 Joint National Priorities, and implementation of Executive Order 13636: Improving Critical Infrastructure Cybersecurity and Executive Order 13650: Improving Chemical Facility Safety and Security.

[*] American Chemistry Council, U.S. Chemical Industry Statistical Handbook 2013 (American Chemistry Council, 2013), http://www.americanchemistry.com/chemistry-industry-facts.

Sector Goals, Priorities, and Activities

As part of this 2015 SSP, the Chemical SCC and GCC identified goals and priorities to guide the sector's security and resilience efforts over the next four years to address the sector's risk profile. The councils then identified 14 activities that partners plan to undertake over the next one to four years, as resources allow. The Chemical Sector aligned its SSP with the national planning framework for security and resilience in the NIPP 2013. As a result, progress toward sector-specific goals, priorities, and activities contributes directly to national achievements under the NIPP 2013. Appendix B demonstrates the detailed alignment of the SSP to NIPP 2013 goals, the Joint National Priorities, and the NIPP 2013 Calls to Action.

Table ES-1. Chemical Sector Goals and Priorities

Goals		Priorities	
1	Identify and assess evolving threats, vulnerabilities, and consequences of the Chemical Sector's physical, cyber, and human elements.	PRIORITY A	Work with local, regional, and national critical infrastructure partners to characterize Chemical Sector risks, address high-risk interdependencies with other sectors, and prioritize risk management activities at the asset and sector level.
2	Strengthen the mechanisms that enable Chemical Sector public-private and cross-sector partnerships and information sharing.	PRIORITY B	Improve Federal Government mechanisms to deliver timely and relevant classified and unclassified information and widely disseminate actionable alerts to Chemical Sector partners.
		PRIORITY C	Promote voluntary sector coordination, secure information sharing through the SCC and GCC, and foster partnerships with the international community to promote a global culture of Chemical Sector security and resilience.
3	Prioritize and sustain cost-effective, risk-based security and resilience programs that increase asset-specific resilience without hindering the economic viability of the sector.	PRIORITY D	Create strategic guidance for owners and operators, coordinate and incentivize voluntary security activities, and jointly develop and promote training and assessment tools or programs for cyber and physical security.
4	Enhance resilience through scientifically sound research and development (R&D) and advance planning and mitigation efforts that ensure rapid response and recovery.	PRIORITY E	Boost training drills, exercises, and risk assessments for cyber and physical security with cross-sector partners and local and regional emergency responders.
		PRIORITY F	Promote R&D projects that provide practical, affordable solutions to improve the sector's resilience.
5	Measure progress and promote continuous learning and adaptation during exercises, incidents, and planning.	PRIORITY G	Share and incorporate best practices and lessons learned from voluntary and regulatory programs into emergency action plans, training, and education programs that support community planning and preparedness initiatives outlined in the Federal Government's 2014 report to the President, *Actions to Improve Chemical Facility Safety and Security – A Shared Commitment*.

Table ES-2. Chemical Sector Activities Mapped to Sector Priorities

Map to Priority		Sector Activities
A D E G	1	Continue to host the Chemical Sector Security Summit through DHS as a primary forum to exchange risk management information and best practices, train sector partners, strengthen public-private networks, and obtain updates on security regulations.
A B C	2	Improve Federal intelligence information sharing through a two-pronged approach: • Share timely Chemical Sector threat information at the non-classified level. • Institute uniform, structured, and coordinated classified briefing sessions that focus on actionable, targeted threat information.
A C	3	Educate DHS and Federal partners on Chemical Sector operations and needs through facility tours and other educational initiatives.
B C	4	Participate in the Global Partnership Chemical Security Sub-Working Group and share relevant information with sector partners.
B E G	5	Conduct targeted outreach and education for small and medium, non-tiered chemical facilities throughout the supply chain.
D G	6	Develop GCC/SCC co-branded advisory and guidance documents.
C E G	7	Raise awareness of cyber threats and available resources.
E G	8	Promote consideration of the use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework to strengthen risk management.
E G	9	Expand training opportunities for Chemical Sector partners based on identified sector risks (including theft and diversion, active shooters, and improvised explosive devices [IEDs]) while engaging SCC partners in planning Federal training and exercises.
E G	10	Work with the critical infrastructure community, DHS, other Federal agencies, and State and local governments to develop a unified credentialing process to ensure Chemical Sector access to facilities and assets in restricted areas following an emergency.
A F	11	Engage owners and operators to identify R&D gaps.
A F	12	Promote large-scale R&D efforts such as Jack Rabbit II to improve and validate scientific risk assessment models with actual event data.
A E G	13	Promote the *Playbook for an Effective All-Hazards Chemical Sector Response* throughout the sector. • Test during National Level Exercises and other drills. • Update as needed following incidents.
G	14	Provide industry with information on Emergency Planning and Community Right-to-Know Act (EPCRA) roles and responsibilities. • Share best practices for facility involvement with Local Emergency Planning Committees and Tribal Emergency Planning Committees.

1 INTRODUCTION

This 2015 Chemical Sector-Specific Plan (SSP) sets the strategic direction for collaborative efforts to improve sector security and resilience over the next four years. It describes how the Chemical Sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (PPD-21). As an annex to the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013), this SSP tailors the strategic guidance provided in the NIPP 2013 to the unique operating conditions and risk landscape of the Chemical Sector. As such, the sector strategy supports the NIPP 2013 national goals and strategy, the 2014 Joint National Priorities (JNPs), implementation of Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636), and Executive Order 13650: Improving Chemical Facility Safety and Security (EO 13650). Public and private sector representatives have identified shared goals and priorities, and a supporting set of collaborative activities they plan to pursue during the next four years, as resources allow.

Sector-Specific Plan development answers NIPP 2013 Call to Action #2, which requires each of the 16 designated critical infrastructure sectors to update their Sector-Specific Plan every four years to reflect joint priorities, address sector reliance on lifeline functions, describe national preparedness efforts, outline cybersecurity efforts, and develop metrics to measure progress. Appendix B illustrates how the Chemical Sector's goals, priorities, and activities support the NIPP 2013 national goals, the five JNPs, and other NIPP 2013 Calls to Action.

This plan describes the Chemical Sector's approach to risk management and national preparedness—considering its distinct assets, operations, and risk profile—in support of Federal plans and directives for security and resilience. The remainder of this Chemical SSP includes the following elements:

- **Chapter 2: Sector Overview**—Provides a view of the sector's assets and operating characteristics, its risk profile, and key public and private sector partners.
- **Chapter 3: Risk Management and National Preparedness**—Describes the mechanisms to achieve sector goals, including ongoing and planned partnership programs, activities, and resources that support the sector's current risk management approach; research and development (R&D) priorities; and how the sector supports national preparedness through incident response and recovery.
- **Chapter 4: Vision, Mission, Goals, and Priorities**—Presents the sector's vision and mission, its updated goals and priorities for chemical security and resilience for the next four years and the specific activities the Chemical Sector public and private sector stakeholders plan to conduct.
- **Chapter 5: Measuring Effectiveness**—Describes the planned approach to measure the effectiveness of individual activities and report on sector progress.

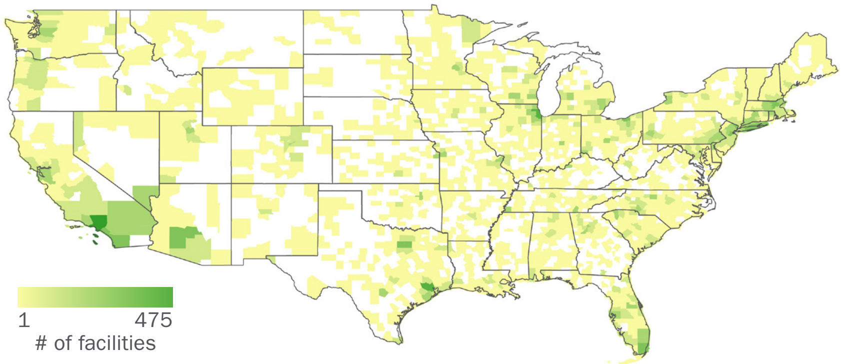
This SSP identifies targets for collaborative planning among the U.S. Department of Homeland Security (DHS), as the Sector-Specific Agency (SSA), and the Chemical Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) members. Partners have a clear and shared interest in ensuring the security and resilience of critical sector assets and this plan represents the collaborative activities that may reduce sector risk and build resilience during the next four years.

2 SECTOR OVERVIEW

2.1 Sector Profile

The Chemical Sector converts various raw materials into more than 70,000 diverse products that are essential to modern life. Several hundred thousand U.S. chemical facilities use, manufacture, store, transport, or deliver chemicals along a complex, global supply chain. Facilities range from petrochemical manufacturers to chemical distributors. End customers include critical infrastructure facilities in several other sectors, which makes the uninterrupted production and transportation of chemicals essential for national and economic security. The following overview provides a snapshot of Chemical Sector assets and operations.

Figure 1: Concentrations of Chemical Sector Facilities in the United States



Chemical facilities are geographically concentrated around coastal ports, positioned for massive importing and exporting of materials and products. This may magnify geographic risks and the effects of local disasters.

Map developed using data from: U.S. Census Bureau, "2013 County Business Patterns," NAICS code 325, last revised April 2015, http://censtats.census.gov/cgi-bin/cbpnaic/cbpsect.pl.

Key Sector Operating Characteristics

Some chemicals, either in their base form or when combined with other chemicals, can cause significant injuries if used maliciously. Sector assets may be appealing targets for attack because of the potential consequences of a toxic release. Chemicals are also appealing targets for theft and diversion to produce weapons of mass destruction (WMD) or improvised explosive devices (IED), or to be used for sabotage or contamination.

The sector has a long history and extensive experience in developing a strong culture of safety and applying security risk management strategies outside of regulatory requirements through the collaborative efforts of professional and industry trade associations, individual chemical companies, and national laboratories.

The majority of Chemical Sector assets are privately owned and operated. However, the highest-risk assets are regulated for security through the DHS Chemical Facility Anti-Terrorism Standards (CFATS) and the Maritime Transportation Security Act (MTSA); the Department of Justice's (DOJ) Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) security rules; and the Department of Transportation's (DOT) Pipeline and Hazardous Materials Safety Administration (PHMSA) safety regulations. Effective security and resilience planning requires a shared commitment between the public and private sectors to implement the most effective risk management strategies throughout the sector.

Chemical manufacturers, warehouses, and distributors can be located great distances from customers, and many chemicals have long supply chains from sourcing to end user. This requires the safe and secure transport of potentially hazardous materials using multiple modes of transportation.

CHEMICAL SECTOR SNAPSHOT

IMPACTS[1]

96% of goods manufactured in the U.S. in 2013 depended on products supplied by the Chemical Sector

866 million tons of chemical products were shipped in 2013

25% of 2013 U.S. GDP was supported by the Chemical Sector

12% of 2013 U.S. Exports were supported by the Chemical Sector

REGULATION

- 3,227 chemical facilities regulated by CFATS as of July 14, 2015[2]
- 3,200 facilities of all types covered by MTSA as of 2013[3]
- 10,500 licensee/permittees subject to ATF security rules as of 2013[4]
- 14,790 shippers covered by DOT security plan and training requirements as of 2014[5]

OWNERS AND OPERATORS

- Chemical Manufacturers
- Petrochemical Manufacturers
- Pharmaceutical Companies
- Agricultural Facilities
- Chemical Distributors
- Universities
- Hardware Stores

FUNCTIONAL AREAS

Manufacturing Plants

Convert raw materials into intermediate and end products

Transport Systems

Transport chemicals to/from manufacturing plants, warehouses, and end users

Warehousing/Storage

Provide downsized repackaging and storage

End Users

Typically consume the chemical purchased

CHEMICAL SEGMENTS

Basic

E.g., Sodium chloride, ethanol, & sulfuric acid

Specialty

E.g., Adhesives, sealants, flavors and fragrances, food additives, & explosives

Pharma-ceutical

E.g., Medicines, biological products, diagnostic substances, & vitamins

Consumer

E.g., Soaps, detergents, bleaches, toothpaste, cosmetics, perfume, & paints

Agricultural

E.g., Fertilizers, pesticides, fungicides, insecticides, & herbicides

CRITICAL SECTOR INTERDEPENDENCIES

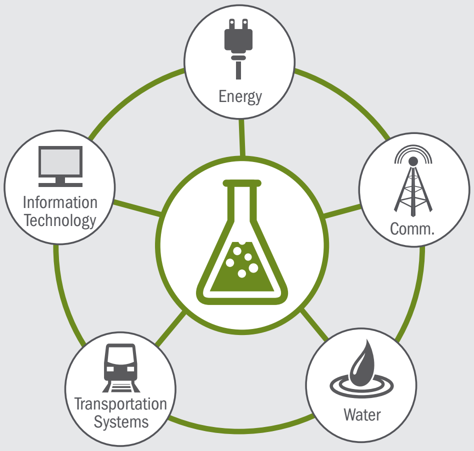
Water—Wastewater treatment and water purification processes rely on chemicals to make water safe, while chemical manufacturing requires large amounts of process and cooling water.

Transportation Systems—Chemicals are transported throughout the country using all modes of transportation. Those modes of transportation rely on petrochemicals and other chemical products.

Communications—Sophisticated communications equipment is used for sector operations and control, while critical communications components are manufactured using chemical products.

Energy—Chemical manufacturing processes can require large amounts of energy, while many energy processes require specialized chemical products (e.g., explosives are essential to mining coal for energy production).

Information Technology—IT systems are a critical component of day-to-day operations; the IT Sector depends on the Chemical Sector for the raw materials used to manufacture components such as computer chips.



2.2 Sector Risks

Facility owners and operators perform individual facility security assessments using state-of-the-art tools developed by professional and industry trade associations, national laboratories, and the Federal Government through public-private coordination. Sector partners also continually share information to identify evolving risks and inform a sector-wide risk profile that forms the basis for the sector's risk management approach and the sector's goals, priorities, and activities.

Some Chemical Sector facilities are covered under a variety of regulatory frameworks from many Federal agencies. While this SSP is focused on the voluntary activities the sector and government partners will pursue over the next four years, progress will continue on implementation of and compliance with regulations. A brief overview of the security regulations some Chemical Sector facilities are covered under is provided in Appendix C.

Notable Trends and Emerging Sector Issues

Since the last SSP was issued in 2010, key changes have affected the sector's risk profile:

- **Increased domestic production of natural gas and shale oil**—Domestic production of natural gas and shale oil has increased dramatically since 2010. Over the next few years, new chemical facilities will be built or expanded to take advantage of the increased domestic supply. Increased domestic supplies of these raw materials will also make the sector less reliant on international sources.
- **Limited information on specific facility threats**—Despite a thorough understanding of sector-wide risks, individual facilities find it difficult to accurately characterize the size and likelihood of evolving threats to specific facilities. This impacts the ability of owners and operators to prioritize security measures that best reduce facility-specific risk.
- **Growing concern of insider threats**—Owners and operators carefully screen employees who have access to large amounts of potentially hazardous materials. However, the sector faces growing concern that a terrorist organization may attempt to radicalize plant employees to compromise or divert chemical assets.
- **Increasingly sophisticated cyber adversaries**—A small portion of process control systems are becoming networked and connected to the Internet for remote monitoring, access control, and ease in uploading patches to system software. Cyber adversaries are simultaneously developing increasingly sophisticated attack capabilities that may exploit this situation.

Significant Chemical Sector Risks

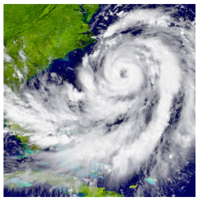
Insider Threat

Cyber and physical security systems in the Chemical Sector largely prevent damage from outsider threats, but the potential for insiders with access to intentionally or unintentionally cause harm is a significant concern in the Chemical Sector. The sector periodically hires third-party, temporary contractors for their specialized experience and expertise. This provides insider access to more individuals who may not have been screened as thoroughly as those employed directly by the facility.

Cyber Threats

Cyber systems in the Chemical Sector, ranging from industrial control systems (ICSs) to large, international secure networks, face a variety of cyber risks, including manmade deliberate attacks, technological failures, human error, and supply chain vulnerabilities. Disruptions to these systems could result in theft of intellectual property; loss of operations capacity; or a chemical theft, diversion, or release. A small portion of ICSs are updated through Internet-accessible systems and third-party devices, which exposes Chemical Sector assets to additional threats from remote attacks.

Natural Disasters and Extreme Weather



Virtually all facilities are susceptible to natural disasters and extreme weather, including tornadoes, fires, earthquakes, and floods, with many facilities located in hurricane-prone areas. The frequency of these events has increased along with the economic impact. These events cause property damage and may affect access to critical resources such as water and electricity, which would adversely affect facility operations and may cause supply chain disruptions.

Deliberate Attacks and Terrorism

Chemical Sector facilities may be a target for attack or terrorism because they hold specific chemicals that could cause significant immediate and long-term damage to people and/or surrounding environments. Materials located at Chemical Sector facilities may also be a target for theft and diversion for use as or in a WMD or IED.

Biohazards and Pandemics

The likelihood of foreign-borne viruses being introduced into the United States' population is increasing, which may bring pandemics that adversely affect the sector's workforce and operations. Many sector partners have plans in place for viruses, such as influenza, that can be adapted to the circumstances of an individual outbreak.

Primary Cross-Sector Interdependencies

The Chemical Sector is closely tied to other critical sector operations, which creates dependencies and interdependencies that could cause a disruption in one sector to affect safe operations in another. The NIPP 2013 identifies lifeline functions—water, transportation systems, communications, and energy—as services and resources that are essential to the operations of most critical infrastructure partners and communities. Identifying lifeline functions, specifically those that are interdependent with other sectors, can help owners and operators prepare for and mitigate the loss of these services in an emergency. While the Chemical Sector may be interdependent in some way with all 16 critical infrastructure sectors, its most significant sector interdependencies are with the lifeline functions, which are listed below and followed by a list of other significant interdependencies and dependencies.

Lifeline Functions: Water, Transportation Systems, Communications, and Energy

Water

Chemical manufacturing requires large amounts of process and cooling water. The Water Sector, which includes drinking water and wastewater systems, is dependent on the Chemical Sector for water purification and sanitation.

Transportation Systems

Transportation systems move inbound raw materials and outbound chemical products via ship, rail, truck, and air. If production facilities are unable to receive raw materials or ship finished products in a timely manner, production may be halted until the raw materials reach a facility or finished materials can be shipped. Transportation systems rely on petrochemicals and other chemical products to maintain operations.

Comm.

Chemical facilities rely on communications to maintain contact with transporters and to conduct day-to-day business operations. Disruptions in the Communications Sector could result in raw material stockpile depletions or large stockpiles of products waiting to be shipped. International business operations could also be limited if individuals are unable to communicate with their counterparts across the globe. Critical communication components are also manufactured using chemical products.

Energy

The Chemical Sector is dependent on the Energy Sector for electricity and critical feedstocks, such as natural gas. An interruption to the power supply would directly affect all chemical facilities located in the impacted region. In addition, the interruption could potentially have a cascading effect on other chemical facilities that are dependent on goods or materials provided by the affected facilities. The Energy Sector is dependent on the Chemical Sector for chemical products (e.g., explosives) to extract coal or perforate gas and oil wells.

Key Interdependencies and Dependencies: Information Technology, Emergency Services, and Food and Agriculture

Information Technology

Information technology is a critical component of day-to-day chemical facility operations, including process control, supply tracking, storage of sensitive information, and automated safety and security systems control. If any of these functions were disrupted, Chemical Sector operations could lose the ability to operate safely and efficiently and secure data. Proprietary information could also be compromised. The Chemical Sector provides chemicals needed for manufacturing electronic components such as microchips and displays.

Emergency Services

Emergency Services are critical when an incident occurs and can help ensure that adverse consequences are minimized. Chemical Sector personnel actively engage emergency services personnel in joint exercises to enhance response efforts.

Food and Agriculture

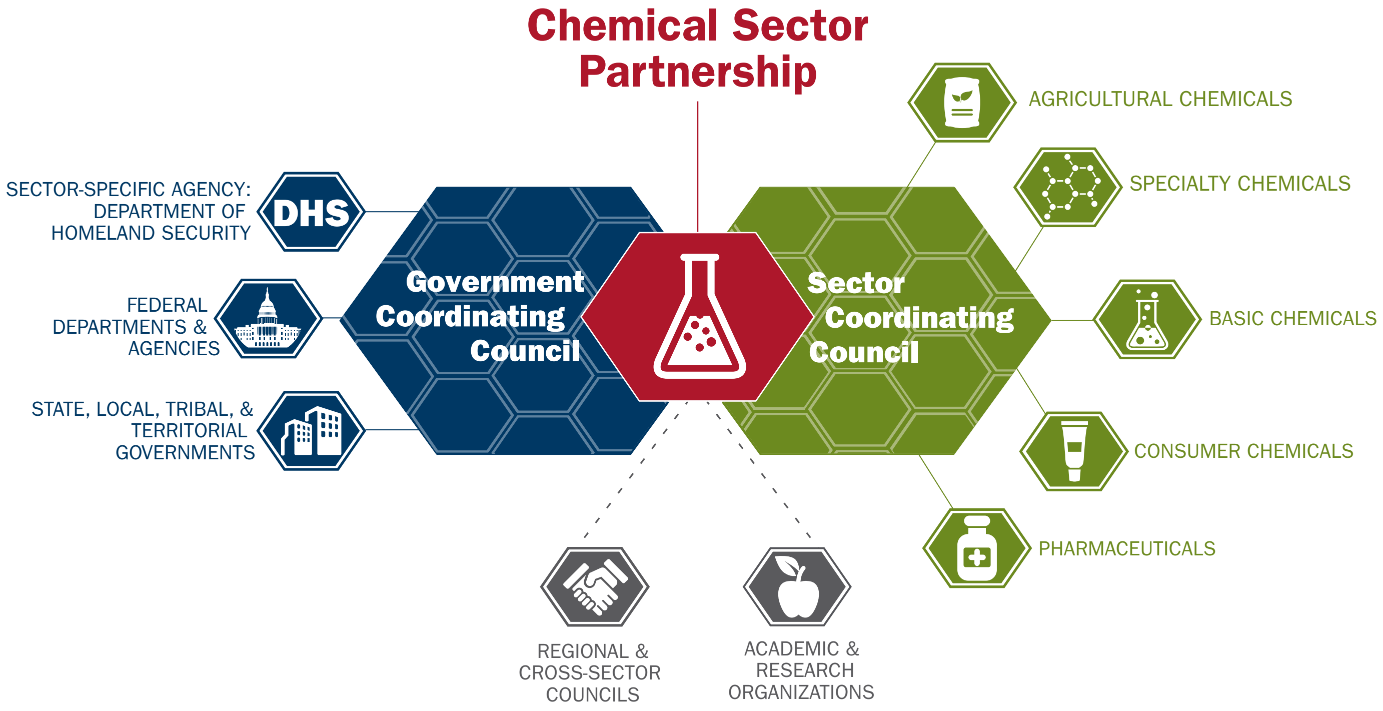
Chemical fertilizers, pesticides, herbicides, and fungicides are all vital components to modern food production. Disruptions to the supply of these chemical products could reduce the amount of food available for consumption.

2.3 Critical Infrastructure Partners

The NIPP 2013 partnership structure includes representative public and private sector councils that operate under the Critical Infrastructure Partnership Advisory Council (CIPAC) construct. This construct facilitates interaction between the community of owners and operators and the sector's Federal, State, local, tribal, and territorial government representatives to conduct deliberations and form consensus positions for the Federal Government.

Chemical Sector Partnership Structure

Figure 2. Chemical Sector Partnership Structure


Chemical Sector Partnership
SECTOR-SPECIFIC AGENCY: DEPARTMENT OF HOMELAND SECURITY
DHS
FEDERAL DEPARTMENTS & AGENCIES
STATE, LOCAL, TRIBAL, & TERRITORIAL GOVERNMENTS
Government Coordinating Council
Sector Coordinating Council
AGRICULTURAL CHEMICALS
SPECIALTY CHEMICALS
BASIC CHEMICALS
CONSUMER CHEMICALS
PHARMACEUTICALS
REGIONAL & CROSS-SECTOR COUNCILS
ACADEMIC & RESEARCH ORGANIZATIONS

The Chemical Sector partnership councils meet regularly to exchange ideas and lessons learned; facilitate sector-level planning and resource allocation; establish effective coordinating structures; and develop security and resilience tools, guidelines, products, and programs.

Chemical Sector-Specific Agency

DHS was designated as the SSA for the Chemical Sector and serves as the lead coordinator of partnership activities and the primary Federal interface for sector-specific security and resilience.

The Office of Infrastructure Protection (IP) fulfills the role of SSA on behalf of DHS. The Assistant Secretary for IP chairs the Chemical GCC and has designated the Director of the Sector Outreach and Programs Division as the representative on behalf of IP. The Director designates an alternate to assist the Director as necessary.

Chemical Sector Coordinating Council

The Chemical SCC is a self-organized, self-governed council of representatives from 15 trade associations representing a high percentage, but not all, of the Nation's Chemical Sector. The Chair and Vice Chair represent individual owners and operators from the trade associations. The Council provides a forum for private companies to coordinate on sector strategy, policy, information sharing, regulations, and risk management activities.

Chemical Government Coordinating Council

The Chemical GCC enables interagency and cross-jurisdictional coordination and communication on chemical security strategies, safety activities, and policies among Federal, State, local, tribal, and territorial government agencies. The GCC also works closely with the SCC to plan, implement, and execute sector-wide resilience and security programs within the Chemical Sector.

A list of GCC and SCC members can be found in Appendix D, and an updated list of council members and their charters can be found at http://www.dhs.gov/chemical-sector-council-charters-and-membership.

CHAPTER ENDNOTES

1. American Chemistry Council, U.S. Chemical Industry Statistical Handbook 2013 (American Chemistry Council, 2013), http://www.americanchemistry.com/chemistry-industry-facts.

2. U.S. Department of Homeland Security, Chemical Facility Anti-Terrorism Standards Fact Sheet, http://www.dhs.gov/publication/cfats-fact-sheet.

3. U.S. Department of Homeland Security, U.S. Coast Guard, "Homeport," accessed February 24, 2015, https://homeport.uscg.mil/mtsa.

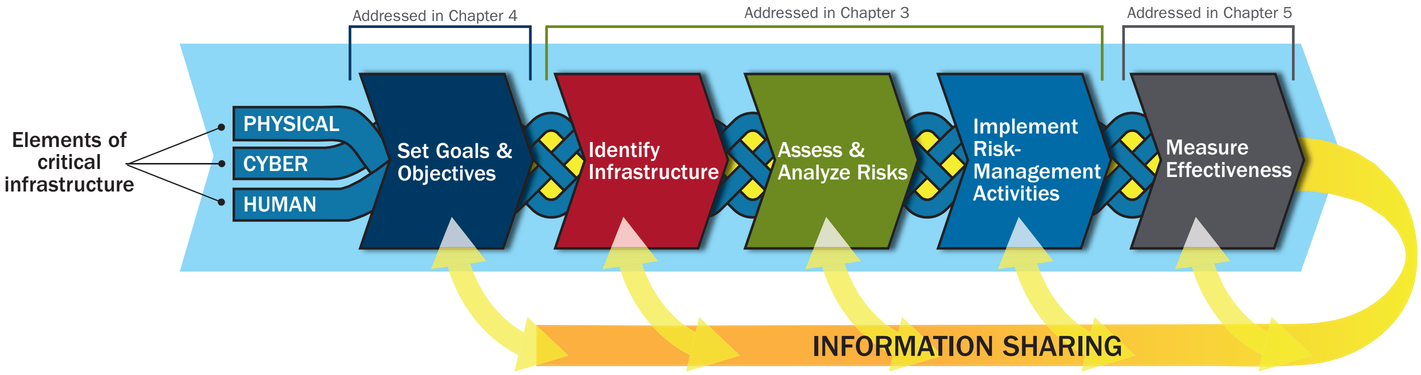
4. U.S. Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives, FY 13 Explosives Inspection Results, https://www.atf.gov/sites/default/files/assets/Explosives/Industry/explosivesfy13.pdf.

5. U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration Hazardous Materials Registration Program, Fiscal Year (FY) 2014 Registration Program Summary Report (PHMSA, 2014), http://phmsa.dot.gov/pv_obj_cache/pv_obj_id_5966C447A679D4259A7F75EAF04326EACD750000/filename/FY2014_Registration_Porgram_Summary_Report_Final_Complete.pdf.

3 RISK MANAGEMENT AND NATIONAL PREPAREDNESS

Risk management is the cornerstone of the NIPP 2013 and the national effort to strengthen security and resilience. It focuses on enabling owners and operators to make risk-informed decisions that best allocate limited resources to the most effective mitigation solutions. The NIPP 2013 critical infrastructure risk management framework (Figure 3) enables the critical infrastructure community to focus on those threats and hazards that are likely to cause harm and to employ prioritized approaches that are designed to prevent or mitigate the effects of those incidents. It also increases security and strengthens resilience by identifying and prioritizing actions to ensure continuity of essential functions and services during incidents and supporting rapid response and restoration.

Figure 3. NIPP 2013 Critical Infrastructure Risk Management Framework



The Chemical Sector goals and priorities are directly rooted in the NIPP 2013 risk management framework and reflect the maturation of the partnership and the significant progress made since the release of the last SSP in 2010. This chapter presents the sector's ongoing efforts and the planned approaches that support risk management and national protection, preparedness, response, recovery, and mitigation following an incident that affects Chemical Sector operations. For more information on sector resources, visit http://www.dhs.gov/chemical-sector or email ChemicalSector@hq.dhs.gov.

3.1 Risk Management

Under the NIPP 2013 risk management framework, risk is the potential for an adverse outcome from an event, determined by the event's likelihood—a function of the specific threats and vulnerabilities—and associated consequences if the event occurs. While individual owners and operators are responsible for managing risk to their individual assets, Chemical Sector partnership activities can improve understanding of threats, vulnerabilities, and consequences and provide owners and operators with tools, guidelines, information, best practices, and resources to facilitate more effective risk assessments and risk management decisions at the facility and sector level.

Owners and operators in the Chemical Sector assess individual risks and establish internal plans to mitigate risks and respond to disruptions. Many facilities are regulated through multiple Federal agencies, and some trade organizations mandate participation in their voluntary risk management programs. Some additional activities undertaken by chemical facilities include conducting internal vulnerability assessments; participating in DHS-sponsored Chemical Sector threat briefings; and collaborating with State, local, regional, territorial, and tribal authorities to build disaster response capabilities.

Identify Infrastructure

DHS works with sector partners to identify assets, systems, and networks that play a vital role in the Nation's security or economy, particularly those that involve significant dependencies, interdependencies, or critical functionality. Drawing largely upon information collected through the CFATS and MTSA regulatory programs, the most critical, highly consequential assets are included in the National Critical Infrastructure Prioritization Program (NCIPP). Due to valuable input from private and public sector partners at the State and local levels and Chemical SSA subject matter experts, the NCIPP also includes chemical facilities that are the sole source of production for important chemicals and critical industry clusters that are geographically important or interdependent due to the use of an important chemical.

Assess and Analyze Risks

Managing and mitigating risk is a cornerstone of critical infrastructure protection and resilience efforts under the NIPP 2013. Risk to an asset, system, or network is a function of the likely consequences of a successful attack, the vulnerability to attack, and the likelihood or threat of an attack. Owners and operators of potentially high-risk chemical facilities are required by regulation to provide information to regulatory agencies to support the performance of security risk assessments at their facilities.

The sector actively promotes numerous SCC trade association voluntary efforts to assess the risk of physical and cyber infrastructure. Most of the SCC member industry associations promote or require, as a condition of membership, vulnerability assessments that have been tailored to their members' needs. Because chemical processes are highly automated, many of these assessments also include cyber vulnerability assessments. In 2009, DHS developed the Voluntary Chemical Assessment Tool (VCAT) for individual companies to identify and prioritize assets. In 2013, DHS decided to move toward a single assessment methodology that would enable comparison across the critical infrastructure community. As a result, DHS no longer offers VCAT. However, the tool is now commercially available, and one of the SCC industry association members purchased a one-year user's license agreement for those companies that found the tool valuable.

RISK ASSESSMENT
Chemical Sector risks can be assessed at the facility and sector level as a function of threats, vulnerabilities, and consequences associated with a particular event. Criteria that may be considered include:

Threat
Natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Vulnerability
Physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

Consequence
Effect of an event, incident, or occurrence.

DHS also regularly provides threat briefings for sector partners in both classified and unclassified environments. Sector partners continue to work together to develop a process that would allow owners and operators to obtain timely and actionable information through these and other information-sharing mechanisms so that the risks can be effectively mitigated.

Implement Risk Management Activities

Sector partners collaborate to develop a number of programs to enhance the security and resilience of the sector. Brief descriptions of these risk management activities are provided in the sections that follow.

Information-Sharing Activities

The **Homeland Security Information Network–Critical Infrastructure** (HSIN–CI) Chemical Sector portal is the primary information-sharing platform for the Chemical Sector. It enables DHS, critical sector security partners, and chemical supply chain professionals to communicate, coordinate, and share information, including when events occur. Primary objectives of HSIN–CI are to generate effective risk management decisions and to encourage collaboration and coordination on plans, strategies, protective measures, and response and recovery efforts among government and owners and operators.

Classified Chemical Sector briefings and **unclassified monthly threat teleconferences** for facility owners and operators, plant managers, and supply chain professionals are hosted by the Chemical SSA. The SSA coordinates with the Federal Intelligence Community to host classified threat briefings for cleared sector partners, while the unclassified monthly teleconference provides an opportunity for DHS to brief the sector on significant changes to the threat environment, results of recent terrorism investigations, and other reported suspicious incidents in both the physical and cyber realm.

The **Chemical Sector Training** and **Chemical Sector Resources** Webpages list the trainings and resources available to sector partners and provide a short synopsis of what is contained in each resource or training. This allows partners to quickly identify the available trainings best suited to their needs.

The Chemical SCC, GCC, and SSA are working to develop and implement an **educational series** to better inform Federal staff about the physical and operational aspects of chemical facilities. The initiative will be launched in 2015 and includes facility tours and operational briefings.

The Chemical SCC, SSA, and GCC are collaboratively developing a **new voluntary initiative to reach small and medium chemical facilities**. The campaign will expand information-sharing capabilities and processes with these facilities using an integrated communication framework and messaging strategies to promote a unified voice for sector security and resilience.

Through the initiative, facilities will have the ability to discover, retrieve, and use accurate, relevant, timely, and actionable threat information. This will inform decision-making and broaden operational capabilities, regardless of a facility's size or specialty. The initiative will accomplish this through activities such as promoting the development of collaborative processes, using integrated resources, identifying existing vulnerabilities, providing resources to mitigate risk and increase resilience, and disseminating chemical educational awareness materials to address unique facility needs.

Additionally, the Chemical SSA is launching a **new initiative specifically designed to bring awareness of the hazards presented by specific chemicals** and promote reporting of suspicious activities regarding the use and purchase of chemicals. This will be done in partnership with the DHS Office of Public Affairs, the See Something, Say Something™ campaign, the Office for Bombing Prevention, the Federal Bureau of Investigation (FBI), and FEMA's America's PrepareAthon. Many Chemical Sector partners also use the See Something, Say Something™ principles at their facilities to look for indicators of an employee's intent to cause harm.

Background checks are still necessary to verify workers' identities, check criminal histories, and validate legal authorization to work. Where appropriate, the sector also relies on Transportation Worker Identification Credential (TWIC) cards to verify that transporters of chemicals have been appropriately vetted, which includes checks for links to terrorist activity.

International Information-Sharing Initiatives

The DHS Office of Infrastructure Protection and the FBI serve as co-chairs of the U.S. Delegation to the **G7 Global Partnership's Chemical Security Sub-Working Group** that was established to improve coordination of nonproliferation-related chemical security programs and assistance activities among Global Partnership member states, the chemical industry, and relevant international and non-governmental organizations. Industry stakeholders are actively engaged in topic discussions for future International Chemical Security Summits, which are modeled after the U.S. Chemical Sector Security Summit.

The sector collaborates with the **U.S. Department of State's Chemical Security Engagement Program** to promote chemical safety and security in the academic, governmental, and industrial sectors and implements scientific engagement capacity-building projects to deter terrorists from acquiring chemicals and chemical expertise to be used to create or enhance a WMD or chemical attack. The Chemical SSA and U.S. Department of State host listening sessions with industry stakeholders to discuss security concerns related to the storage, production, and transportation of chemicals outside the United States.

DHS serves as the Chair of the **Chemical Security Working Group of the Critical Five**, which provides a platform for critical infrastructure-related information sharing between the governments of Australia, Canada, New Zealand, the United Kingdom, and the United States.

Training Seminars and Exercises

IP has developed a no-cost series of six Web-based **security awareness courses** to train and educate a broad range of individuals, including public and private sector managers and employees, critical infrastructure owners and operators, government partners at all levels, and the general public. These courses provide guidance on how to improve security in the workplace, prevent and prepare for potential active shooter incidents, notice and report suspicious purchases and activities, identify and take action against insider threats to critical infrastructure, spot theft and diversion threats and vulnerabilities, and detect and report suspicious activities associated with adversarial surveillance. These cross-sector courses replaced the Web-based Chemical Security Awareness Training Program.

The **Security Seminar and Workshop Series** encourages facility owners and operators and their security partners to collaborate in an interactive seminar and discussion forum. The outcomes of this collaboration include progress in information sharing about all-hazards threats, vulnerabilities, and consequences, as well as enhanced communication between facilities and their local emergency response teams.

Tabletop exercises, sponsored through the Chemical SSA and SCC, are unclassified, adaptable exercises that create an opportunity for public and private critical infrastructure stakeholders and their public safety partners to address gaps, threats, issues, and concerns with incident response and recovery. The various exercises contain a number of incident-specific resources as well as the suite of documents needed to conduct a Homeland Security Exercise and Evaluation Program compliant tabletop exercise.

"Theft and Diversion – What You Can Do," a Web-based course, introduces critical infrastructure personnel to information needed to identify and take action to prevent the theft and diversion of resources, raw materials, technologies, and products. This course provides an overview of theft and diversion activities, the indicators associated with them, and actions that employees can take to report and prevent them.

The DHS ***Vehicle Inspection Guide and Video*** helps private and public sector partners to mitigate risk from vehicle-borne IEDs and strengthen critical infrastructure resilience by providing a step-by-step explanation of how to conduct a thorough vehicle inspection systematically, efficiently, and safely. The video covers the interview of vehicle occupants and a detailed systematic vehicle inspection in greater detail, focusing on indicators of suspicious behavior. In addition, the guide provides vital knowledge of "hot spots" and "IED indicators" for multiple types of vehicles. To request a copy of the guide and video, send an email to ChemicalSector@hq.dhs.gov.

Chemical Sector Security Summit

The annual Chemical Sector Security Summit (the Summit) is an industry-wide networking and educational event co-sponsored each year by DHS and the Chemical SCC. A diverse group of attendees participates every year, consisting of top-level government and private sector leaders, including DHS officials, congressional staff, and senior government officials from Federal agencies; international participants; and members of the national media. The Summit provides a forum for representatives from the chemical community to share and exchange information, network with other security professionals, share best practices and lessons learned, learn about chemical security regulations, and gain insight into the roles of State, local, and Federal agencies and departments involved with chemical security. The Summit also offers participants free educational workshops and trainings on a variety of security-related topics such as CFATS updates, hazardous material safety, theft and diversion, and supply chain resilience.

3.2 Managing Cyber Risks

While chemical facilities ultimately manage cybersecurity risks at a company and facility level, developing sector-wide risk reduction tools and capabilities can provide major long-term benefits. Working together, sector partners have developed strategies, tools, trainings, workshops, and programs that promote cybersecurity awareness and increase Chemical Sector cybersecurity knowledge and capabilities:

- **Cyber-Dependent Infrastructure Identification**—The Chemical SCC established a working group with the Oil and Natural Gas Subsector to identify cyber-critical assets called for by EO 13636. While the sector did not identify any assets that met the criteria for cyber-critical assets under Cyber-Dependent Infrastructure Identification, the Chemical Sector is now well positioned to conduct a sector-wide risk assessment of cyber and physical risks.
- **Critical Infrastructure Cyber Community (C^3) Voluntary Program**—Sector partners are participating in the C^3 Voluntary Program to promote sector awareness and adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. As part of this effort, DHS is coordinating with sector partners to develop a Chemical Sector Framework Implementation Guide driven by the NIST Cybersecurity Framework. The guidance document will include best practices to improve cybersecurity at chemical facilities.
- **Partnership-Developed Cybersecurity Resources**—Owners and operators have worked with DHS and other Chemical Sector partners to develop a DVD containing sector-specific tools and resources, including security measures guides, guidance on building the business case for cybersecurity investments, and tabletop training exercises for owners and operators.

- **Cyber Storm Exercises and Preparedness**—Chemical Sector partners actively participate in national Cyber Storm exercises to strengthen cyber preparedness in both the public and private sectors. This provides an opportunity to test the Chemical Sector cyber incident response and crisis communication processes and identify areas for improvement. The sector is currently pilot testing an Information Sharing and Analysis Center (ISAC) to facilitate the dissemination of cyber threat data between DHS, other government agencies, and the Chemical Sector. The ISAC is scheduled to be fully operational by mid-2015 and will be managed by one of the SCC industry association members.

- **Workshops, Presentations, and Webinars**—The DHS Office of Cybersecurity and Communications (CS&C), in collaboration with the Chemical SSA, hosts cybersecurity workshops and presentations at the annual Chemical Sector Security Summit, in addition to many trade association conferences. The Office of Cybersecurity and Communications also hosts cybersecurity Webinars to enhance general cybersecurity education by sharing relevant, specific, and reported cyber threats. Topics and objectives are determined through continued outreach to DHS components and private sector critical infrastructure partners.

- **Trade Association Programs**—Trade associations within the Chemical Sector offer programs that focus specifically on information technology trends within the chemical industry. These voluntary programs provide assessment and management tools for their member companies, and some trade associations host annual conferences for chemical information technology professionals to share best practices.

- **Working Groups**—DHS facilitates a number of working groups to foster information sharing, promote cybersecurity awareness, and help better coordinate cyber risk management activities. The Chemical Sector participates in the Cross-Sector Cybersecurity Working Group (CSCSWG), which enhances cybersecurity protection efforts by identifying opportunities to improve cross-sector coordination, highlighting cyber dependencies and interdependencies, and sharing cybersecurity products and findings.

- **CFATS Risk-Based Performance Standards (RBPS)**—One of the 18 RBPS established under CFATS, RBPS 8, requires high-risk chemical facilities to address cybersecurity in order to deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls, such as supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), process control systems (PCSs), industrial control systems (ICSs), critical business systems, and other sensitive computerized systems. RBPS 8 is consistent with the NIST Cybersecurity Framework. The RBPS Guidance provides potential security considerations and optional security measures for facilities to consider when seeking to comply with RBPS 8. The RBPS Guidance document is available online to all facilities and may be used as a tool to help strengthen even unregulated facilities' cyber risk management processes.

3.3 Mitigating Disruption from the Loss of Lifeline Functions

The Chemical Sector is tightly integrated with the Water, Transportation Systems, Communications, and Energy Sectors. Addressing critical dependencies requires active engagement and information sharing with cross-sector security partners to identify complementary risk management practices, programs, and R&D projects that can improve local and regional resilience and mitigate consequences from the loss of lifeline functions.

Owners and operators develop contingency plans, backup power generation (if available), alternate communications methods, transportation routes, and modes of transportation as part of their emergency operations and business continuity plans. In particular, owners and operators draw upon lessons learned from cross-sector partners during Federal, State, and local emergency exercises to form more accurate expectations of lifeline function availability during a major disaster.

For facilities that desire assistance with developing continuity plans, DHS developed and distributes a Business Continuity Planning (BCP) Suite that enables businesses to create, improve, or update their business continuity plans. This product helps companies of any size to develop and unify multiple plans across their organizations, better enabling them to review and test their business continuity program. The Suite consists of three main components: a BCP training module, automated BCP and disaster recovery plan (DRP) generators, and a self-directed exercise for testing an implemented BCP.

3.4 Research and Development Priorities

Science and technology offer considerable promise in helping to develop efficient and cost-effective ways of mapping potential consequences, identifying potential threats, assessing risk and vulnerability, and enhancing the protective posture of Chemical Sector infrastructure. A focused R&D program will help DHS and its partners enhance the security of the Chemical Sector. Many cross-cutting R&D efforts exist within DHS, other Federal agencies, academia, and international partners. The Chemical Sector identified the following R&D activities:

- **Development of economic models**—In order to assess the economic consequences to the Nation from a terrorist attack, accident, or naturally occurring event on the chemical supply chain, the Chemical Sector needs a model that will calculate the relative risk to the national economy analogous to the human health consequences model. Risk results should be reported both in terms of health impact and economic impact and be as comprehensive as possible to include cradle-to-grave issues.

- **International dependence and interdependence of the Chemical Sector**—After decades of decreased domestic manufacturing capabilities, the U.S. chemical industry is investing in domestic manufacturing due to the increased domestic production of oil and natural gas. The U.S. chemical industry still relies on offshore manufacturing due to many factors, including additional domestic regulations and their associated costs, increased labor and raw materials costs, and the lack of synergy among multiple regulations that affect the industry's ability to maintain profitability within the United States. The industry needs a study that will help it understand the impacts and repercussions these trends might have on national security. The study needs to identify the countries with which the United States is developing dependencies regarding chemical supply chain issues and determine the criticality of these dependencies.

- **Better understanding of and updates to the toxicological and dispersion data being used to determine the hazardous nature of certain chemicals**—The Chemical Sector seeks to revisit toxicological data to reexamine their origins and determine if better data are available or perform testing and analysis where data are lacking. This updated data will help improve sophisticated models to understand how chemicals disperse when released—specifically dense gases.

- **Analysis and decision support methods that can be used to identify cascading effects of individual or multipoint attacks or natural disasters**—Given the highly interconnected nature of the Nation's infrastructure, attacks on one or more parts of infrastructure may cause cascading effects that are not easily revealed through the standard consequence assessment. Analysis and decision support systems that help model the cascading effects of attacks on chemical infrastructure, the infrastructure that depends on the Chemical Sector, and the infrastructure on which the Chemical Sector is dependent would help provide more accurate assessment of potential consequences and an informed allocation of resources.

The Chemical SCC works closely with the Chemical SSA to ensure that technologies developed in research settings meet their needs, are used operationally, and are available throughout the sector.

The *National Critical Infrastructure Security and Resilience Research and Development Plan* (National CISR R&D Plan) identified five cross-sector R&D priority areas that are intended to inform R&D investments, promote innovation, and guide research across the critical infrastructure community. The Chemical Sector will consider these five priority areas as inputs in its planning efforts to align its R&D activities and support implementation of the National CISR R&D Plan.

3.5 Chemical Sector National Preparedness Efforts

The five National Planning Frameworks—established under the National Preparedness Goal, the cornerstone for the implementation of the Presidential Policy Directive 8: National Preparedness (PPD-8)—foster a shared understanding of roles and responsibilities across critical infrastructure sectors to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk.

Chemical Sector partners are active participants in the National Level Exercises designed to test and assess a coordinated response in order to improve the preparedness and resilience of both the sector and the Nation. The Chemical SSA invites industry partners to participate in the National Level Exercises overview that discusses the background, objectives, overarching scenarios, tentative dates, and level of involvement for private sector partners. During the exercise, the Chemical SSA is stationed in the Master Control Cell, while sector partners participate in overall exercise activities as indicated in the exercise scenario and sector objectives. At the conclusion of the exercise, Chemical Sector participants develop an after-action report that informs the sector's standard operating procedure (SOP) for responding to all hazards, as well as the Federal after-action report.

The Chemical Sector contributes to disaster response and recovery when chemicals are involved in the following ways:

- Companies participating in voluntary security programs sponsored by industry trade associations engage in a number of community outreach and emergency preparedness activities to build strong working relationships with local communities and other stakeholders. Activities include participation in Community Advisory Panels and open houses. To help prepare for an emergency, member companies invite local fire departments and emergency response teams to participate in emergency response drills at their facilities. These outreach efforts help the community better understand company activities and allow companies to hear stakeholders' concerns.

- The Chemical Transportation Emergency Center (CHEMTREC) provides chemical-specific and general assistance during emergencies and around-the-clock access to hazardous material safety information to fire fighters, law enforcement officials, and other emergency responders. If needed, teams of experts can be dispatched to the site of an incident to provide further assistance with the response and recovery.

- The Chemical Security Analysis Center (CSAC) offers "CSAC Reachback" to Federal, State, local, tribal, territorial, and first-responder agencies. CSAC provides around-the-clock subject matter expert analyses to ensure robust science and technology-based responses to questions posed by DHS and other Federal agencies regarding the threat or hazard posed by a specific chemical.

- In addition to joint drills with local first responders, many sector partners also participate and support Transportation Community Awareness and Emergency Response (TRANSCAER) events designed to prepare first responders and communities in case of a hazardous materials (HAZMAT) emergency.

- The Chemical SCC, in collaboration with the SSA, developed *Playbook for an Effective All-Hazards Chemical Sector Response*. This SOP serves to fulfill the sector's commitment to safety, security, and resilience during an emergency. The SOP also provides a more effective process for the Chemical Sector and DHS to strengthen their partnership in relation to critical infrastructure resilience.

- CFATS- and MTSA-regulated facilities are required to address response and preparedness activities. CFATS facilities, in accordance with RBPS 9, develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders. MTSA-regulated facilities must conduct drills and exercises to increase and test the proficiency of facility personnel assigned with security duties and the proficiency of the established security program.

4 VISION, MISSION, GOALS, AND PRIORITIES

An effective Chemical Sector partnership is instrumental in achieving a vision shared by Chemical Sector asset owners, government and community partners, and regulators. The Chemical SCC and government partners collectively developed five joint goals for sector security and resilience and seven priorities to pursue over the next four years. These goals and priorities directly support the Joint National Priorities and the NIPP 2013 Calls to Action.

CHEMICAL SECTOR VISION

An economically competitive and increasingly resilient industry that achieves and maintains a sustainable security posture by effectively reducing vulnerabilities to and consequences of all hazards, using risk-based assessments, industry best practices, and a comprehensive information-sharing environment between industry and government.

CHEMICAL SECTOR MISSION

Reduce the Nation's chemical manufacturing and distribution infrastructure's vulnerability to all hazards based upon sound risk-based methodologies.

Table 1. Chemical Sector Goals and Priorities

Goals		Priorities	
1	Identify and assess evolving threats, vulnerabilities, and consequences of the Chemical Sector's physical, cyber, and human elements.	PRIORITY A	Work with local, regional, and national critical infrastructure partners to characterize Chemical Sector risks, address high-risk interdependencies with other sectors, and prioritize risk management activities at the asset and sector level.
2	Strengthen the mechanisms that enable Chemical Sector public-private and cross-sector partnerships and information sharing.	PRIORITY B	Improve Federal Government mechanisms to deliver timely and relevant classified and unclassified information and widely disseminate actionable alerts to Chemical Sector partners.
		PRIORITY C	Promote voluntary sector coordination, secure information sharing through the SCC and GCC, and foster partnerships with the international community to promote a global culture of Chemical Sector security and resilience.
3	Prioritize and sustain cost-effective, risk-based security and resilience programs that increase asset-specific resilience without hindering the economic viability of the sector.	PRIORITY D	Create strategic guidance for owners and operators, coordinate and incentivize voluntary security activities, and jointly develop and promote training and assessment tools or programs for cyber and physical security.

Goals		Priorities	
4	Enhance resilience through scientifically sound R&D and advance planning and mitigation efforts that ensure rapid response and recovery.	PRIORITY E	Boost training drills, exercises, and risk assessments for cyber and physical security with cross-sector partners and local and regional emergency responders.
		PRIORITY F	Promote R&D projects that provide practical, affordable solutions to improve the sector's resilience.
5	Measure progress and promote continuous learning and adaptation during exercises, incidents, and planning.	PRIORITY G	Share and incorporate best practices and lessons learned from voluntary and regulatory programs into emergency action plans, training, and education programs that support community planning and preparedness initiatives outlined in the Federal Government's 2014 report to the President, *Actions to Improve Chemical Facility Safety and Security – A Shared Commitment*.

4.1 Chemical Sector Activities

Chemical Sector partners developed a set of 14 activities that they can collaboratively conduct to effectively implement this SSP and meaningfully contribute to sector goals and priorities. The following activities include both voluntary partnership activities and tasks the sector may pursue over the next one to four years. While the SSPs are updated every four years, the Chemical Sector partnership may update its activities more frequently to reflect evolving risk, changing resource allocations, and progress or completion.

Sector partners are operating in resource-limited environments, and moving forward on any of the identified activities will depend largely on resource availability, budgets, and sector-wide prioritization processes. Rather than constrain priorities and activities based on available resources alone, the sector identified the top activities it believes will make a significant contribution to national security and resilience. The GCC and SCC will meet annually to update, prioritize, and build on the SSP activities.

Table 2. Chemical Sector Activities Mapped to Sector Priorities

Map to Priority		Sector Activities
A D E G	1	Continue to host the Chemical Sector Security Summit through DHS as a primary forum to exchange risk management information and best practices, train sector partners, strengthen public-private networks, and obtain updates on security regulations.
A B C	2	Improve Federal intelligence information sharing through a two-pronged approach: • Share timely Chemical Sector threat information at the non-classified level. • Institute uniform, structured, and coordinated classified briefing sessions that focus on actionable, targeted threat information.
A C	3	Educate DHS and Federal partners on Chemical Sector operations and needs through facility tours and other educational initiatives.

Map to Priority	Sector Activities	
B C	4	Participate in the Global Partnership Chemical Security Sub-Working Group and share relevant information with sector partners.
B E G	5	Conduct targeted outreach and education for small and medium, non-tiered chemical facilities throughout the supply chain.
D G	6	Develop GCC/SCC co-branded advisory and guidance documents.
C E G	7	Raise awareness of cyber threats and available resources.
E G	8	Promote consideration of the use of the NIST Cybersecurity Framework to strengthen risk management.
E G	9	Expand training opportunities for Chemical Sector partners based on identified sector risks (including theft and diversion, active shooters, and IEDs) while engaging SCC partners in planning Federal training and exercises.
E G	10	Work with the critical infrastructure community, DHS, other Federal agencies, and State and local governments to develop a unified credentialing process to ensure Chemical Sector access to facilities and assets in restricted areas following an emergency.
A F	11	Engage owners and operators to identify R&D gaps.
A F	12	Promote large-scale R&D efforts such as Jack Rabbit II to improve and validate scientific risk assessment models with actual event data.
A E G	13	Promote the *Playbook for an Effective All-Hazards Chemical Sector Response* throughout the sector. • Test during National Level Exercises and other drills. • Update as needed following incidents.
G	14	Provide industry with information on Emergency Planning and Community Right-to-Know Act (EPCRA) roles and responsibilities. • Share best practices for facility involvement with Local Emergency Planning Committees and Tribal Emergency Planning Committees.

5 MEASURING EFFECTIVENESS

Owners and operators use a variety of ways to measure progress toward improving security and increasing resilience through internal risk assessment and management processes at the facility level. Measuring improvements in security and resilience at the sector level is far more difficult. Where possible, sector partners attempt to measure how their voluntary partnership activities contribute to risk reduction and enhanced resilience across the sector.

As the SSA, DHS has the primary responsibility for measuring and reporting progress toward sector activities using relevant metrics. An established performance metrics system designed to track the progress of sector activities is used to ensure accurate and consistent measurement.

Table 3 aligns Chemical Sector activities with a set of possible performance metrics that the SSA may use to measure and report progress, where possible. The metrics not only measure the completion of an activity—using output measures such as the number of products developed or partners engaged—but also aim to measure the outcomes of these activities—particularly how effective they are in achieving progress toward sector goals.

Within the voluntary sector partnership, often the best available outcome measure is to track intent to act based on the information, tools, or guidance received through sector activities. The SSA measures this intent to act using a survey—during or following each engagement or activity—that asks three things:

- Was the information they received current and relevant?
- Will the information inform decision-making?
- Will participants further share the information within their organization?

Survey results indicate the effectiveness of each activity in equipping participants with the information, tools, guidance, and processes to take actions that ultimately reduce or better manage sector risk.

The SSA will report sector progress through the National Annual Report and the quadrennial SSP updates. The following list is not exhaustive of all possible ways to measure effectiveness, and sector asset owners may voluntarily measure and report additional information on sector progress during the National Annual Reporting process.

Table 3. Chemical Sector Activities and Expected Metrics

	Chemical Sector Activities	Expected Metrics
1	Continue to host the Chemical Sector Security Summit through DHS as a primary forum to exchange risk management information and best practices, train sector partners, strengthen public-private networks, and obtain updates on security regulations.	• Level of participation at the Chemical Sector Security Summit • Change in level of participation at the Summit over time • How participants intend to use the information they received during the Summit
2	Improve Federal intelligence information sharing through a two-pronged approach: • Share timely Chemical Sector threat information at the non-classified level. • Institute uniform, structured, and coordinated classified briefing sessions that focus on actionable, targeted threat information.	• Number of products developed • Number of classified threat briefings held • Number of products distributed to stakeholders • Method used for distribution of products • Level of participation in classified threat briefings • Change in threat briefings participation over time • How recipients or participants intend to use the information received

	Chemical Sector Activities	Expected Metrics
3	Educate DHS and Federal partners on Chemical Sector operations and needs through facility tours and other educational initiatives.	• Number of facility tours offered by private sector partners • Number of tours attended by DHS and other Federal agencies
4	Participate in the Global Partnership Chemical Security Sub-Working Group and share relevant information with sector partners.	• Number of Global Partnership Chemical Security Sub-Working Groups attended • Level of participation in the Working Group • Change in participation in the Working Group over time • Information products developed • Number of products distributed to stakeholders • Method used for distribution of products
5	Conduct targeted outreach and education for small and medium, non-tiered chemical facilities throughout the supply chain.	• Number of information products and education training products developed • Number of information products and education training products distributed to small and medium, non-tiered facilities • How recipients intend to use the information received
6	Develop GCC/SCC co-branded advisory and guidance documents.	• Number of guidance documents developed • Number of guidance documents distributed to stakeholders • Method used to distribute guidance documents • How recipients intend to use the information
7	Raise awareness of cyber threats and available resources.	• Number of information products developed • Number of information products distributed to stakeholders • Meetings and workshops organized or coordinated by the sector to share information and training on cyber threat • How recipients and participants intend to use the information
8	Promote consideration of the use of the NIST Cybersecurity Framework to strengthen risk management.	• Meetings and workshops organized and coordinated to promote implementation of the NIST Cybersecurity Framework • Development and distribution of best practice guidance • How recipients and participants intend to use the information they receive
9	Expand training opportunities for Chemical Sector partners based on identified sector risks (including theft and diversion, active shooters, and IEDs) while engaging SCC partners in planning Federal training and exercises.	• Number of workshops and trainings held • Change in participation in workshops and trainings over time • How participants intend to use the information they receive

	Chemical Sector Activities	Expected Metrics
10	Work with the critical infrastructure community, DHS, other Federal agencies, and State and local governments to develop a unified credentialing process to ensure Chemical Sector access to facilities and assets in restricted areas following an emergency.	• Status of developing a unified credentialing process
11	Engage owners and operators to identify R&D gaps.	• Meetings and working groups organized and coordinated to identify R&D gaps • Number of R&D gaps identified
12	Promote large-scale R&D efforts such as Jack Rabbit II to improve and validate scientific risk assessment models with actual event data.	• Number of workshops, Webinars, and events • Level of participation in workshops, Webinars, and events • How participants intend to use the information they receive
13	Promote the *Playbook for an Effective All-Hazards Chemical Sector Response* throughout the sector. • Test during National Level Exercises and other drills. • Update as needed following incidents.	• Information products developed to promote the *Playbook for an Effective All-Hazards Chemical Sector Response* • Meetings and workshops organized and coordinated to promote the *Playbook for an Effective All-Hazards Chemical Sector Response* • How recipients and participants intend to use the information they receive • Participation in National Level Exercises
14	Provide industry with information on Emergency Planning and Community Right-to-Know Act (EPCRA) roles and responsibilities. • Share best practices for facility involvement with Local Emergency Planning Committees and Tribal Emergency Planning Committees.	• Number of information products developed and distributed • Number of best practices products and tools developed and distributed • Method used for distribution of products • How recipients intend to use the information received

APPENDIX A
Acronyms and Terms

AN	ammonium nitrate
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BCP	business continuity planning
CBP	U.S. Customs and Border Protection
CFATS	Chemical Facility Anti-Terrorism Standards
CHEMTREC	Chemical Transportation Emergency Response Center
COTP	Captain of the Port
CSAC	Chemical Security Analysis Center
CSCSWG	Cross-Sector Cybersecurity Working Group
CWC	Chemical Weapons Convention
DCS	distributed control system
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOC	Department of Commerce
DOJ	Department of Justice
DOL	Department of Labor
DOS	Department of State
DOT	Department of Transportation
DRP	Disaster Recovery Plan
EAP	Expedited Approval Program
EO 13636	Executive Order 13636: Improving Critical Infrastructure Cybersecurity
EO 13650	Executive Order 13650: Improving Chemical Facility Safety and Security
EPA	Environmental Protection Agency
EPCRA	Emergency Planning and Community Right-to-Know Act
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSP	Facility Security Plan
GCC	Government Coordinating Council
GDP	gross domestic product
HAZMAT	hazardous materials
HMTA	Hazardous Materials Transportation Act
HSIN	Homeland Security Information Network
HSIN-CI	Homeland Security Information Network – Critical Infrastructure
ICS	industrial control system
IED	improvised explosive device
ISAC	Information Sharing and Analysis Center
IP	DHS Office of Infrastructure Protection
JNPs	Joint National Priorities
MARSEC	maritime security
MSRAM	Maritime Security Risk Assessment Model
MTSA	Maritime Transportation Security Act
NCIPP	National Critical Infrastructure Prioritization Program
NIPP 2013	*National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*
NIST	National Institute of Standards and Technology
PCS	process control system
PHMSA	Pipeline and Hazardous Materials Safety Administration
PPD	Presidential Policy Directive
PPD-8	Presidential Policy Directive 8: National Preparedness
PPD-21	Presidential Policy Directive 21: Critical Infrastructure Security and Resilience
R&D	research and development
RBPS	Risk-Based Performance Standards
RSSM	Rail Security-Sensitive Materials
SCADA	supervisory control and data acquisition
SCC	Sector Coordinating Council
SOP	standard operating procedure
SSA	Sector-Specific Agency
SSI	Sensitive Security Information
SSP	Sector-Specific Plan
SVA	Site Vulnerability Assessment
TRANSCAER	Transportation Community Awareness and Emergency Response
TSA	Transportation Safety Administration
USDA	U.S. Department of Agriculture
VCAT	Voluntary Chemical Assessment Tool
WMD	weapon of mass destruction

APPENDIX B
Alignment with the NIPP 2013

This appendix illustrates the alignment of Chemical Sector priorities with the NIPP 2013 national goals and Joint National Priorities, and the ways in which sector activities contribute to the NIPP 2013 Calls to Action.

Table B-1. Chemical Sector Priorities Aligned with Joint National Priorities and NIPP Goals

Chemical Sector Priorities	Joint National Priorities					NIPP Goals
	Strengthen Management of Cyber and Physical Risks to Critical Infrastructure	Build Capabilities and Coordination for Enhanced Incident Response and Recovery	Strengthen Collaboration Across Sectors, Jurisdictions, & Disciplines	Enhance Effectiveness in Resilience Decision-making	Share Information to Improve Prevention, Protection, Mitigation, Response, & Recovery Activities	
A Characterize Sector Risks	PRIORITY A		PRIORITY A	PRIORITY A		Assess and analyze risks to critical infrastructure (including threats, vulnerabilities, and consequences) to inform risk-management activities.
B Improve Federal Government Information-Sharing Mechanisms				PRIORITY B	PRIORITY B	Share information across the critical infrastructure community to build awareness and enable risk-informed decision-making.
C Promote Voluntary Sector Coordination			PRIORITY C	PRIORITY C		
D Jointly Develop Training Tools for Cyber and Physical Security	PRIORITY D		PRIORITY D			Secure critical infrastructure against physical, cyber, and human threats through sustainable risk reduction efforts, while considering costs and benefits.
E Encourage Drills with Emergency Responders		PRIORITY E	PRIORITY E			Enhance critical infrastructure resilience by minimizing consequences and employing effective response and recovery.
F Support Research and Development (R&D) Efforts to Improve Chemical Sector Resilience	PRIORITY F				PRIORITY F	
G Share and Incorporate Best Practices	PRIORITY G				PRIORITY G	Promote learning and adaptation during and after incidents and exercises.

Table B-2. Contribution of the Chemical Sector Activities to the NIPP 2013 Calls to Action

Chemical Sector Contribution or Aligned Activity		NIPP 2013 Calls to Action											
		#1	#2	#3	#4	#5	#6	#7	#8	#9	#10	#11	#12
1	Continue to host the Chemical Sector Security Summit through DHS as a primary forum to exchange risk management information and best practices, train sector partners, strengthen public-private networks, and obtain updates on security regulations.					X				X			
2	Improve Federal intelligence information sharing through a two-pronged approach: • Share timely Chemical Sector threat information at the non-classified level. • Institute uniform, structured, and coordinated classified briefing sessions that focus on actionable, targeted threat information.					X				X			
3	Educate DHS and Federal partners on Chemical Sector operations and needs through facility tours and other educational initiatives.					X				X			
4	Participate in the Global Partnership Chemical Security Sub-Working Group and share relevant information with sector partners.			X		X	X	X					
5	Conduct targeted outreach and education for small and medium non-tiered chemical facilities throughout the supply chain.			X		X				X			
6	Develop GCC/SCC co-branded advisory and guidance documents.			X		X				X			
7	Raise awareness of cyber threats and available resources.				X	X							
8	Promote consideration of the use of the NIST Cybersecurity Framework to strengthen risk management.				X	X				X			
9	Expand training opportunities for Chemical Sector partners based on identified sector risks (including theft and diversion, active shooters, and IEDs) and engage SCC partners in planning Federal training and exercises.						X	X		X			
10	Work with the critical infrastructure community, DHS, other Federal agencies, and State and local governments to develop a unified credentialing process to ensure Chemical Sector access to facilities and assets in restricted areas following an emergency.			X				X	X	X			X
11	Engage owners and operators to identify R&D gaps.				X						X		
12	Promote large-scale R&D efforts such as Jack Rabbit II to improve and validate scientific risk assessment models with actual event data.					X					X		
13	Promote the *Playbook for an Effective All-Hazards Chemical Sector Response* throughout the sector. • Test during National Level Exercises and other drills. • Update as needed following incidents.					X	X	X		X			X
14	Provide industry with information on Emergency Planning and Community Right-to-Know Act (EPCRA) roles and responsibilities. • Share best practices for facility involvement with Local Emergency Planning Committees and Tribal Emergency Planning Committees.			X						X			
	Chemical Sector goals and priorities were developed in alignment with the 2014 Joint National Priorities in support of Call to Action #1.	X											
	Development of the 2015 Chemical Sector-Specific Plan meets Call to Action #2.		X										
	The Chemical Sector supports Call to Action #10 by working with its Federal partners to implement the *National Critical Infrastructure Security and Resilience Research and Development Plan*.										X		
	The measurement approach outlined in Chapter 5: Measuring Effectiveness will enable the Chemical Sector to evaluate and report on the progress of partnership efforts in support of Call to Action #11.											X	

NIPP 2013 Calls to Action

Call to Action #1: Set National Focus through Jointly Developed Priorities

Call to Action #2: Determine Collective Actions through Joint Planning Efforts

Call to Action #3: Empower Local and Regional Partnerships to Build Capacity Nationally

Call to Action #4: Leverage Incentives to Advance Security and Resilience

Call to Action #5: Enable Risk-Informed Decision-making through Enhanced Situational Awareness

Call to Action #6: Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects

Call to Action #7: Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents

Call to Action #8: Promote Infrastructure, Community, and Regional Recovery Following Incidents

Call to Action #9: Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education

Call to Action #10: Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions

Call to Action #11: Evaluate Progress Toward the Achievement of Goals

Call to Action #12: Learn and Adapt During and After Exercises and Incidents

APPENDIX C
Federal Security Authorities

Executive Order 13650: Improving Chemical Facility Safety and Security

Executive Order 13650: Improving Chemical Facility Safety and Security directs the Federal Government to improve operational coordination with State and local partners; improve Federal agency coordination and information sharing; modernize policies, regulations, and standards; and work with stakeholders to identify best practices. The working group tasked with implementing this Executive Order includes the U.S. Department of Homeland Security (DHS), U.S. Department of Agriculture (USDA), U.S. Department of Justice (DOJ), U.S. Department of Labor (DOL), U.S. Department of Transportation (DOT), and the Environmental Protection Agency (EPA). The working group released a 2014 report to the President entitled *Actions to Improve Chemical Facility Safety and Security—A Shared Commitment* that outlines the Federal Government's plan for moving forward on five thematic areas, which will impact all Federal security authorities as they relate to the Chemical Sector. More information about Executive Order 13650 can be found at https://www.osha.gov/chemicalexecutiveorder/.

Department of Homeland Security Authorities

Chemical Facility Anti-Terrorism Standards (CFATS)

DHS developed the Chemical Facility Anti-Terrorism Standards (CFATS), to implement its authority to regulate security at chemical facilities designated by CFATS as high-risk. Under CFATS, DHS has authority to require high-risk chemical facilities to complete Security Vulnerability Assessments (SVAs), develop Site Security Plans, and implement the protective measures necessary to meet the Risk-Based Performance Standards (RBPS) established by DHS. On December 18, 2014, the President signed into law the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (the CFATS Act of 2014). The Act re-codifies and reauthorizes the CFATS program and adds new provisions, while preserving most of the existing CFATS regulations. More information about CFATS can be found at http://www.dhs.gov/chemical-facility-anti-terrorism-standards.

One of the new provisions in the CFATS Act of 2014 requires DHS to establish an Expedited Approval Program (EAP) as a voluntary option for high-risk chemical facilities assigned a final tier level of 3 or 4 to develop and submit Site Security Plans. The CFATS Act directed DHS to issue guidance that "identifies specific security measures that are sufficient to meet the risk-based performance standards" for facilities that choose to submit a Site Security Plan pursuant to the EAP. This Guidance—and the prescriptive measures contained in the Guidance—are intended explicitly to apply to facilities that elect to participate in the EAP. The security posture of facilities submitting Site Security Plans and Alternative Security Plans through the regular, non-prescriptive Site Security Plan/Alternative Security Plan process will continue to be evaluated against the RBPS in a holistic fashion. DHS will not apply the EAP Guidance in a prescriptive fashion to the Site Security Plans and Alternative Security Plans in the regular CFATS approval process.

The EAP Guidance is available online to all chemical facilities. Facilities not covered by the regulations may consider reviewing the guidance and implementing some of the measures to strengthen security at their site.

Ammonium Nitrate Security Program

DHS has proposed Ammonium Nitrate (AN) Security Program regulations to reduce the likelihood of a terrorist attack involving misused AN. The proposed AN Security Program would require AN sellers to register, maintain AN sales records, and report potential thefts/losses of AN; encourage AN sellers to report any suspicious orders of AN; require AN purchasers to register; and make registration for both sellers and purchasers involve screening against the Terrorist Screening Database. DHS is currently developing the final rule. More information about the AN Security Program can be found at http://www.dhs.gov/ammonium-nitrate-security-program.

Maritime Transportation Security Act (MTSA)

Under MTSA, chemicals transported by ship and chemical facilities adjacent to navigable waterways are required to perform a vulnerability assessment and develop a Facility Security Plan (FSP), which must be approved by the local captain of the port (COTP). FSPs must include security measures; procedures for responding to security threats; and detailed preparedness, prevention, and response activities for each maritime security (MARSEC) level. High-risk vessels must also submit security assessments and security plans. The COTP and port stakeholders use the Maritime Security Risk Assessment Model (MSRAM) to perform detailed scenario risk assessments on all critical industry facilities at the local port level. The model also provides the capability to compare different targets and geographic areas at the national, regional, and local levels. More information about MTSA can be found at https://homeport.uscg.mil/mtsa.

Rail Transportation Security

The Transportation Security Administration (TSA) is responsible for security requirements for rail transportation, covering freight railroad carriers and rail operations at certain, fixed-site facilities that ship or receive specified hazardous materials (HAZMAT) by rail, known as rail security-sensitive materials (RSSM). The rule codifies the scope of TSA's existing inspection program that requires regulated parties to allow TSA and other DHS officials to enter, inspect, and test property, facilities, and records relevant to rail security. This rule also requires parties to designate rail security coordinators and report significant security concerns to DHS. Freight rail carriers and certain facilities handling RSSM must have procedures in place to report location and shipping information to TSA upon request and within a specific time frame. Regulated entities must also implement chain-of-custody requirements to ensure a positive and secure exchange of RSSM. TSA also proposed to clarify and extend the sensitive security information (SSI) protections to cover certain information associated with rail transportation. More information about the Rail Transportation Security rule can be found at http://www.tsa.gov/stakeholders/standards-and-regulations-1.

Hazardous Materials Transportation Act (HMTA)

TSA, in conjunction with DOT, is required to administer safeguards for licensing HAZMAT transport drivers. Under the rules developed by TSA, the roughly 3.5 million commercial drivers with HAZMAT endorsements on their commercial driver's licenses are required to undergo a periodic security assessment based on a review of FBI criminal records and immigration and other relevant international databases, as appropriate. More information about the HMTA can be found at http://www.tsa.gov/stakeholders/enrollment-0.

Trade Act of 2002

U.S. Customs and Border Protection (CBP) is required to collect electronic cargo information from all modes of commercial transport prior to the arrival of the cargo in or departures from the United States. The information required must be sufficient to enable CBP to identify high-risk shipments. The regulations require advance transmission of electronic cargo information to CBP by way of a CBP-approved electronic data interchange system. Such information must include the actual chemical name (not brand name) or the United Nations HAZMAT code identifier number for all shipments of chemicals and HAZMAT. This information assists DHS in tracking the movement of HAZMAT in order to ensure cargo safety and security. More information about CBP's role in HAZMAT can be found at http://www.cbp.gov/border-security/ports-entry/cargo-security/cargo-control/enforce-tsa.

Department of Justice Authorities

Controlled Substances Act

The Drug Enforcement Administration (DEA) established regulations for the registration and security of 34 controlled essential (List 1) and precursor (List 2) chemicals. Manufacturers and distributors (including importers and exporters) of the 34 identified chemicals must establish controls to guard against theft and diversion, maintain records of all transactions, and report suspicious orders for these chemicals to DEA. DEA evaluates the effectiveness of List 1 facilities' respective physical security, sales, and storage procedures. More information about DEA's security requirements can be found at http://www.deadiversion.usdoj.gov/pubs/manuals/sec/general_sec.htm.

Federal Explosives Laws

The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) licenses manufacturers, dealers, and importers of explosives, and issues permits for users of explosives. Manufacturers, as well as other licensees and permittees, must submit to ATF the names and identifying information of responsible persons and employees. These individuals must then undergo criminal history background checks. Convicted felons, aliens, and other prohibited persons are disqualified from serving as responsible persons in the business or possessing explosives.

The Federal Explosives Laws also require all persons, including manufacturers, to comply with the Federal explosives storage requirements that set forth the standards of public safety and security necessary to protect against explosives thefts, accidental explosions, and other safety and security hazards. For example, magazines must meet certain construction requirements, bullet-proof standards, and table of distances specifications (e.g., explosive materials must be located a safe distance from public highways and inhabited dwellings). Additionally, manufacturers and other regulated entities must submit to ATF onsite inspections, maintain records of all explosives transactions, and report all thefts and losses of explosives. They must also submit product samples on request by ATF. More information about Federal Explosives Laws can be found at https://www.atf.gov/content/Explosives/explosives-enforcement.

Department of Transportation Authorities

Federal Rail Safety

Rail carriers are required to compile annual data on certain shipments of explosive, toxic by inhalation, and radioactive materials. This data will be used to analyze safety and security risks along rail routes where those materials are transported, assess alternative routing options, and make routing decisions based on those assessments. Rail carriers are responsible for addressing security plan issues related to en route storage and delays in transit, and inspecting placarded hazardous materials (HAZMAT) rail cars for signs of tampering or suspicious items, including improvised explosive devices (IEDs). More information about the Federal Rail Safety regulations can be found at https://www.fra.dot.gov/Page/P0010.

Hazardous Materials Transportation Act

DOT has established regulations governing the transportation of HAZMAT on public highways, by rail, in aircraft, and in vessels. These regulations cover classification, packaging, emergency communication, training, and modal-specific requirements. Among DOT's rules are those that require sellers and transporters of certain types of HAZMAT to develop and implement security plans and conduct security training for employees. Security plans must be based on vulnerability assessments and must address personnel, access, and en route security related to HAZMAT in transportation. DOT ensures the Nation's HAZMAT transportation rules are uniform through its preemptive authority over non-Federal requirements. DOT serves as the U.S. authority for HAZMAT transportation safety and security in international forums. DOT also has authority over the operational aspects of the vehicles used to carry HAZMAT. DOT rules prohibit States from issuing, renewing, transferring, or upgrading a commercial driver's license with a HAZMAT endorsement unless the TSA has first conducted a fingerprint-based records assessment of the applicant and determined that the applicant does not pose a security risk warranting denial of the HAZMAT endorsement. DOT also requires States establish a HAZMAT endorsement renewal period of no more than five years to ensure each holder of a HAZMAT endorsement routinely and uniformly receives a security screening. More information about these regulations can be found at http://phmsa.dot.gov/regulations.

Department of Commerce Authorities

Export Administration Regulations

Department of Commerce (DOC) regulates the export of dual-use items (i.e., items with both commercial and potential military uses), including those covered by the Chemical Weapons Convention (CWC) under the Export Administration Regulations. DOC also regulates the export of other chemicals and related equipment and technology of proliferation concern as controlled by the Australia Group. More information about the Export Administration Regulations can be found at http://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear.

Chemical Weapons Convention (CWC) Implementation Act of 1988

The CWC Implementation Act authorizes the collection of information on certain activities involving chemicals covered by the CWC, as well as onsite inspections by the Organization for the Prohibition of Chemical Weapons (OPCW). The OPCW is the international organization responsible for administering and verifying CWC compliance worldwide. DOC's CWC Regulations require facilities involved in CWC-covered activities and chemicals at specific threshold amounts to submit annual declarations and reports, and to submit to onsite inspections. The declarations contain information on quantities produced, processed, consumed, exported, and/or imported by the facility. More information about the CWC can be found at http://www.cwc.gov/index.html.

Department of State Authorities

International Traffic in Arms Regulations

The Department of State (DOS) regulates the export of munitions items, which include certain chemical weapons agents and their immediate precursors covered by the CWC, under the International Traffic in Arms Regulations. Additionally, DOS, as the U.S. National Authority, is responsible for otherwise ensuring U.S. compliance with the CWC. More information about the CWC can be found at http://www.cwc.gov/index.html.

APPENDIX D
Sector Council Membership

Chemical Sector Government Coordinating Council Members

U.S. Department of Commerce

U.S. Department of Homeland Security

U.S. Department of Justice

U.S. Department of Transportation

U.S. Environmental Protection Agency

Chemical Sector Coordinating Council Industry Association Members

Agricultural Retailers Association

American Chemistry Council

American Coatings Association

American Fuel and Petrochemical Manufacturers

American Petroleum Institute

The Chlorine Institute

Compressed Gas Association

Council of Producers & Distributors of Agrotechnology

CropLife America

The Fertilizer Institute

International Institute of Ammonia Refrigeration

International Liquid Terminals Association

Institute of Makers of Explosives

National Association of Chemical Distributors

Society of Chemical Manufacturers & Affiliates

Up-to-date member lists and charters of the Chemical Sector Coordinating Council and Government Coordinating Council can be found at http://www.dhs.gov/chemical-sector-council-charters-and-membership.

Homeland
Security