CHEMICAL SECTOR
COORDINATING COUNCIL

Playbook for an Effective All-Hazards Chemical Sector Response

A Publication developed by the Chemical Sector Coordinating Council in partnership with the Cybersecurity and Infrastructure Security Agency

Fifth Edition, August 2022

Page intentionally blank

Acknowledgments

The development of the *Playbook for an Effective All-Hazards Chemical Sector Response* was led by the Chemical Sector Coordinating Council (SCC) in conjunction with the U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), Stakeholder Engagement Division (SED), as the Chemical Sector Risk Management Agency (SRMA).

Distribution

This document is available on the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) Chemical Sector. The HSIN-CI Chemical Sector within HSIN allows for information sharing among federal, state, and local agencies and private sector owners and operators. For additional distribution information and access requirements for the HSIN-CI Chemical Sector Portal, contact Chemicalsector@cisa.dhs.gov.

Notice

This document does not constitute a regulatory requirement, nor is it intended to conflict, replace, or supersede existing regulatory requirements or create any enforcement standard. The information in this document is intended solely as guidance. This document is not intended for, nor can it be utilized for the purpose of creating any rights enforceable by any party in litigation.

Contents

INTRODUCTION

This Handbook provides a standard operating procedure (SOP) to assist the Chemical Sector[1] in preparing for, responding to, and recovering from an all-hazards emergency. The intended audience for this SOP is the Chemical Sector Coordinating Council (SCC) membership and the Cybersecurity and Infrastructure Security Agency (CISA) as the Chemical Sector Risk Management Agency (SRMA).

This SOP is developed pursuant to the sector partnership model described in the National Infrastructure Protection Plan (National Plan) and is designed to implement the concept of operations described in the National Response Framework (NRF).[2] This SOP defines the respective roles and responsibilities of the Chemical SCC and the Chemical SRMA as well as their interaction in support of a coordinated public-private sector response to an all-hazards emergency.[3]

This SOP also describes actions intended to assist the Chemical SRMA in support of its responsibility to inform and make recommendations to senior government officials regarding Chemical Sector impacts and needs requirements as part of the federal response to an all-hazards emergency.[4] For purposes of this SOP, all-hazards emergencies can be classified as either a forecasted (advance-notice) or a non-forecasted (no-notice) event. The specific nature of the emergency will determine the appropriate course of action as outlined in this SOP.

This SOP was developed as a collaborative effort between the Chemical SCC and the Chemical SRMA. Contents reflect many of the lessons learned over years of experience with joint exercise activities and real-world emergencies that required a coordinated public-private sector response. While it is designed to provide as much specific guidance as possible, this SOP is also intended to be dynamic, flexible, and tailored in its application to accommodate the unique aspects of an emergency scenario; as well as the unique authorities, capabilities, and decision-making processes of the various partner organizations that must work together to affect a well-coordinated response.

Finally, this SOP is intended to support the close communication and coordination between the leadership of the Chemical SCC and the Chemical SRMA that is critical to the effectiveness of an all-hazards response.

Target Audience

This Handbook was developed specifically to help communication between members of the Chemical Sector Coordinating Council and the CISA Chemical Sector Risk Management Agency.

[1] The Chemical Sector is characterized in the Chemical Sector-Specific Plan and includes four major segments: (1) basic chemistry, (2) specialty chemicals, (3) agricultural chemicals, and (4) consumer products. All in all, several hundred thousand facilities in the United States use, manufacture, store, repackage, distribute, transport, or deliver chemicals, encompassing everything from petroleum refineries, pharmaceutical manufacturers, to hardware stores. The facilities that make up the Chemical Sector typically belong to one of four key functional areas: (1) manufacturing plants, (2) transport systems, (3) warehousing and storage systems, and (4) chemical end users.

[2] Critical infrastructure sector leadership (SRMAs, GCCs, and SCCs) create an established network to collaborate with their respective private sector partners and support cross-sector response operations. https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf (accessed March 2022).

[3] In the context of this SOP, an "all-hazards emergency" can include a natural disaster or a severe weather event, such as a hurricane, tornado, flood, winter weather, or earthquake, or a naturally occurring event, such as a pandemic outbreak. It can also include a manmade intentional act, such as a physical terrorist attack or cyberattack, or an unintentional manmade act, such as a hazardous materials release, an industrial accident, or facility technology failure.

[4] It should be noted this SOP is not intended to be all-inclusive of the roles and responsibilities of the Chemical SRMA during an all-hazards response. The Chemical SRMA has numerous internal obligations that outline its additional interagency roles and responsibilities regarding incident response.

SECTION 1: PURPOSE

This SOP is intended to:

- Assist the Chemical Sector in preparing for, responding to, and recovering from all-hazards emergencies that require a coordinated response between government and the organizations that comprise the Chemical SCC.
- Establish a protocol providing for effective two-way incident communication and coordination and establishing situational awareness between the Chemical Sector (via the Chemical SCC) and the Federal Government (via CISA as the Chemical SRMA).
- Define the respective roles and responsibilities and the interaction required between the Chemical SCC and the Chemical SRMA in the context of an emergent threat or incident in progress—in alignment with the National Incident Management System (NIMS) and the NRF.
- Identify key elements of information and assistance needed by the Chemical Sector in all-hazards emergency situations to provide timely, accurate, and actionable information to Chemical SCC members.
- Provide the Chemical SRMA with national- and regional-level Chemical Sector-specific information and situational awareness during all-hazards emergencies.
- Enable the communication and coordination of specific prevention, protection and mitigation, response, and recovery actions pertinent to the Chemical Sector during all-hazards emergencies via the partnership between the Chemical SRMA and Chemical SCC.

SECTION 2: SCOPE

The scope of this SOP includes slow-onset (advance-notice) and no-notice all-hazards emergency events that trigger a coordinated government/Chemical SCC response.

- The processes described in this SOP utilize the unified risk-based approach and partnership model for "steady-state" protection detailed in the National Plan.
- Chemical Sector requirements generated by the threat or incident at hand are coordinated through NRF and NIMS organizational structures. This applies to activities in the local incident area, as well as response and recovery activities outside the local incident area, regionally or nationally.

SECTION 3: ROLES AND RESPONSIBILITIES

This section describes the respective general roles and responsibilities of the various public and private Chemical Sector partners in the context of an all-hazards emergency event that triggers a coordinated government/Chemical SCC response.

Chemical Sector Coordinating Council

- Establish and maintain communications with members/employees regarding preparedness actions prior to an event (including national and international Chemical Sector association resources/data).
- Gather information on impacts, requests for information (RFIs), and requests for assistance (RFAs) during the response to and recovery from an event.[5]
- Encourage members to establish and maintain contact with state, local, tribal, and territorial (SLTT) agencies prior to incidents and submit RFIs/RFAs best handled locally to the appropriate SLTT agency.
- Forward information from CISA regarding the scheduling/convening of sector-specific and cross-sector calls and situational awareness updates posted on HSIN-CI to the Chemical SCC membership and owner/operator community.
- Provide the Chemical SRMA and the Chemical SCC leadership (generally via e-mail) with a synopsis of event impacts on their members/employees and corresponding response actions, as well as any RFIs/RFAs made by SCC members (whether made to local authorities, CISA Central, or elsewhere).
- Conduct sector-specific teleconference calls among Chemical SCC leadership co-chairs.
- Provide a synopsis of event preparedness prior to impact, subsequent impacts on their members/employees, and corresponding response actions, as well as any RFIs/RFAs made by SCC members (whether made to local authorities, CISA Central, or elsewhere), during cross-sector incident teleconference calls sponsored by CISA.
- The SCC can coordinate the sharing and development of best practices and dissemination of intelligence for longer term incidents.

Chemical Sector Risk Management Agency

- Receive information about an actual or emerging incident that could affect one of the critical infrastructure sectors for which CISA serves as the SRMA.
- Coordinate with the Office of Chemical Security, the Chemical Facility Anti-Terrorism Standards (CFATS) team, Regional Partners, and DHS Headquarters to determine course of action.
- Aggregate incident information and engage with the appropriate sector partners to validate preliminary assumptions and initial assessments.
- Determine the potential level of impacts based on the Incident Severity Schema for physical and cyber incidents (see Table 1).
- Determine the appropriate sector-related actions and level of effort:
    - Maintain situational awareness and coordinate with sector partners through the established collaboration structures:

[5] Refer to Appendix C for emergency event-related RFIs/RFAs.

        - HSIN-CI: Chemical Community of Interest (COI)
        - Ad-Hoc Classified Briefings
        - Ad-Hoc Conference Calls
        - Joint SCC/GCC Meetings
        - Classified Threat Briefings
        - Unclassified Threat Briefings
    - Share information with sector stakeholders according to established protocols and information-sharing mechanisms.
    - Create weekly written briefs that will advise SCC of potential “advance notice events” so that they are on the radar to raise awareness and visibility for the sector.
    - Conduct stakeholder engagements (including Chemical SCC membership and national and international Chemical Sector associations, as appropriate).
    - Manage RFIs/RFAs to and from sector stakeholders.
- Support U.S. Department of Homeland Security (DHS) and interagency reporting requirements.
- Manage and make available emergency event-related information on HSIN-CI Chemical Sector.
- Collect information from Chemical Sector stakeholders (including Chemical SCC membership and national and international Chemical Sector associations) regarding sector impacts and corresponding prevention, protection, mitigation, response, and recovery actions, and report these to CISA Central via national incident reporting mechanisms (see Appendix E) and to the Chemical SCC leadership.
- Facilitate Chemical Sector access to federally produced pre- and post-event impact analysis and modeling via CISA Central.
- Coordinate with the SCC leadership on the need for and the scheduling/convening of sector-specific teleconferences to foster situational awareness.
- Co-chair sector-specific teleconferences along with the SCC leadership.
- Notify the SCC leadership of the scheduling/convening of cross-sector teleconference calls.
- Provide the SCC with information summaries regarding sector-specific and cross-sector teleconference calls.
- Leverage cross-sector capabilities of CISA’s Emergency Support Function #14 (ESF #14) for information gathering, sharing, and identification of potential or actual cross-sector impacts.

Table 1. Incident Severity Schema

Incident Severity Schema	
Physical or Cyber Incident Severity	Incident Severity Schema Description
Level 5 – *Emergency* (Black)	Poses an imminent threat to the provision of wide-scale critical infrastructure services, national government stability, or the lives of U.S. persons
Level 4 – *Severe* (Red)	Likely to result in a significant impact to critical infrastructure across multiple sectors/regions for a sustained period
Level 3 – *High* (Orange)	Likely to result in a demonstrable impact on critical infrastructure function/operability across sectors/regions for a sustained period
Level 2 – *Medium* (Yellow)	May have an impact on critical infrastructure function/operability across sectors/regions for a sustained period
Level 2 – *Low* (Green)	Unlikely to have an impact on critical infrastructure function/operability for a sustained period
Level 0 – *Baseline* (White)	Unsubstantiated or inconsequential event involving infrastructure assets

SECTION 4: STANDARD OPERATING PROCEDURE

This SOP applies to both slow-onset (advance-notice) events as well as no-notice events that trigger a coordinated government/SCC response.[6]

- **Slow-onset or advance-notice events** can be forecasted more than 72 hours prior to impact and allow for incident-specific planning and preparation. Examples include a hurricane, a major winter storm, a forecasted major flood, or a tracked wildfire encroaching on a populated area resulting in evacuation orders. This can also apply to new or emerging risks of concern, such as a developing pandemic, or political unrest forecasted for a specific date.
- **No-notice events** occur suddenly with little to no warning, thus limiting the ability to prepare in advance. Examples include a natural disaster (e.g., tornado, earthquake, or sudden and unpredictable wildfire), an industrial accident, or a man-made/intentional act of sabotage or terrorism resulting in a cyber incident and/or infrastructure failure.

The type of incident will also affect the incident management phase. Table 2 below outlines the relationship between the types of events and the phases.

Table 2. Advance-Notice and No-Notice Events and Incident Management Phases

Incident Type	Incident Management Phase	Response Timing
Slow-Onset or Advance-Notice Events	*Phase 1: Guarded*	*72–96 hours prior to impact*
	Phase 2: Concern	*48–72 hours prior to impact*
No-Notice Events	*Phase 3: Urgent*	*Less than 48 hours' notice or no warning*

Physical vs. Cyber Incidents

As the SRMA, CISA will maintain its responsibilities for information sharing, stakeholder engagement, responses to RFIs and RFAs, and internal coordination, even when incidents fall short of thresholds that require a coordinated federal response (e.g., a severity determination below Level 3 on the Cyber Incident Severity Schema). This allows for the SCC to receive notices of incidents that fall short of thresholds that require federal response as it will assist with proactive responses to deal with various local/regional supply chain issues and support.

[6] Most forecasted events take the form of weather-related or seasonal/cyclical phenomena such as hurricanes, severe flooding, wildfires, ice storms, etc. The Chemical SCC leadership should be actively engaged with the Chemical SRMA in determining whether a coordinated response to the event is needed based on the information available.

These activities may include headquarters personnel communicating and sharing information with sector partners and regional office personnel working directly with affected facilities. Absent a coordinated federal response, CISA Central maintains 24–7 watch operations and share information with the SRMA management team and the regional offices through established protocols. Both physical and cyber incident information pertinent to the sector flow through CISA Central. RFIs and RFAs for incidents (physical and cyber) are routed and managed through CISA Central and may relate to various topics, including those listed in Table 3 to the right.

When appropriate the Chemical SRMA will coordinate with SRMA Governance and the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) team to ensure critical infrastructure and cyber incidents are reported appropriately.

For significant incidents that require a coordinated federal response, CISA Central acts as the national coordinating center providing situational awareness and integrated actionable information for incidents affecting physical infrastructure as set forth in Presidential Policy Directive 21 (PPD-21): *Critical Infrastructure Security and Resilience*. CISA Central collects information from and shares information with the SRMA management teams and the regional offices, which serve as conduits of information between the center and sector stakeholders. The SRMA management teams and the regional offices use their established information-sharing mechanisms to coordinate with sector stakeholders. The centers may host subject matter experts (SMEs) from the SRMA management team as part of their day-to-day operations, as appropriate.

CISA Central evaluates incident severity and the results of the evaluation inform CISA's decision to further activate incident management activities, as shown in Table 4 below.

Table 3. Potential Topics for RFIs and RFAs from Sector Stakeholders

General/Pre-Incident
• **Threats:** Emergent or imminent threats that could affect operations of critical infrastructure or endanger the safety of personnel or the public • **Adversaries:** Antagonists that sponsor, support, and/or carry out attacks or exploitation on U.S. critical infrastructure • **Suspicious Activities and Behaviors:** Characteristics of suspicious activities related to attack or exploitation operations • **Motivation and Intent:** Apparent ambitions behind adversaries' actions • **Indicators:** Signs that an attack or exploitation is underway or escalating • **Locations and targets:** Sectors, subsectors, industries, geographic regions, and types of systems/knowledge/data adversaries are targeting • **Assets:** Equipment, supplies, or personnel used by adversaries to conduct attacks or exploitation • **Methods, capabilities, and activities:** Tactics, techniques, and procedures adversaries use to launch and implement attacks or exploitation
Incident-Specific
• **Impacts:** Critical infrastructure operations, capabilities, or supply chains compromised by attack or exploitation • **Cascading Impacts:** An attack's indirect effects on facilities, sectors, and communities that are not the primary target(s) • **Status:** Operational condition of affected facilities, including expected time of restoration • **Coordination:** Organization between critical infrastructure partners • **Access:** Procedures to enter the affected area

Table 4. SRMA Activation in Physical vs. Cyber Incidents

Activation Step	Physical	Cyber
Inform	Affected entities may submit incident information through the SRMA management team, through a regional office, or directly to CISA Central.	Affected entities may submit incident information through the SRMA management team, through a regional office, or directly to CISA Central. Affected entities are encouraged to contact CISA Central directly for asset response.
Validate	CISA Central assesses the severity of the incident against established criteria, assessing both physical and cyber impacts, and informs CISA leadership.	CISA Central provides severity assessment in coordination with counterparts and shares information, as appropriate, with CISA Central and CISA leadership. CISA Central and CISA leadership assess both cyber and physical impacts.
Activate	CISA leadership determine the appropriate level of response based on the information available. Sector-specific incident management and coordination activities may involve the direct participation of multiple elements across the organization, depending on the type of incident, its severity, and the need for a coordinated federal response.	

Incident Management and Coordination Practices

To effectively support incident management and coordination, the Chemical SCC and SRMA conduct administrative and operational practices across three stages of incident management:

- **Preparedness**: Update contact information, read and monitor key resources and channels, and integrate continual process improvement into preparation plans and activities.
- **Response**: Review, monitor, contribute to, and share analysis of advance-notice and no-notice events, as well as facilitate coordinated response activities with industry and government partners.
- **Recovery**: Monitor and ensure the flow of up-to-date information, facilitate communication between appropriate partners, and support the transition back to steady-state operations.

Preparedness

The Chemical SCC and Chemical SRMA should undertake various collaborative activities, including the conduct of joint communications drills and periodic joint refresher training and exercises for members of the SCC, prior to the onset of a regular hazard season/cycle (e.g., hurricane, wildfire, tornado, flood, winter storm seasons/cycles, as appropriate).

In addition to communications drills, training, and exercise activities, the Chemical SCC and Chemical SRMA should collaborate to accomplish the following prior to the onset of a predictable hazard season/cycle:

- Update Chemical SCC, Chemical SRMA, and other agency contact lists such as CFATS, CISA Central, etc.
- Key sector points of contact information.
- Association and state chemical council contact information.

- Individual Chemical SCC member organization/Chemical SRMA call trees (see Appendix A for a list of Chemical Sector contacts).
- Review this SOP and solicit input on improvements/lessons learned.
- HSIN-CI reminder (to update password; see Appendix F regarding HSIN).
- Anticipate potential incident management needs/issues.
- Review (and disseminate to Chemical SCC membership, as appropriate) pre-season/pre-cycle impacts analysis and modeling provided by the National Infrastructure Simulation and Analysis Center (NISAC) and hazard modeling provided by Federal Emergency Management Agency (FEMA), when available.[7]
- Enroll in Government Emergency Telecommunications Services (GETS) Program.
- Work with partners to identify critical facilities, assets, functions, and interdependencies to reduce risk pre- and post-event.
- Identify changes to relevant statutory and/or regulatory programs, potential capabilities, and/or limiting factors pertaining to recovery support for infrastructure systems.
- Review relevant changes to CISA (or other federal, state, or local department/agency) policies, plans, and procedures with potential impact on sector information sharing and incident response capabilities/activities.
- Establish awareness of industry emergency shut-down processes and related needs (see Appendix G for a list of actions supporting preparedness planning).

Response

Trigger Point for Phase Increase of Advance-Notice Events:

- An advance-notice event is one that can be forecasted more than 72 hours prior to impact. Examples include a hurricane, a major winter storm, a forecasted major flood, or a wildfire encroaching into a populated area.
- For an advance-notice event, CISA, in consultation with FEMA, will determine whether the event is sufficient to trigger activating this SOP. The Chemical SRMA will notify the Chemical SCC leadership of the need to initiate this SOP at the Phase 1 level.

Trigger Point for Phase Increase for No-Notice Events:

- No-notice events are sudden with little-to-no warning, thus limiting the ability to prepare in advance. These types of events can take the form of a natural disaster, such as a tornado or earthquake; an industrial accident; or a manmade/intentional act of sabotage or terrorism resulting in a cyberattack and/or infrastructure failure. Response to a no-notice event at the federal level will be incident-specific. Once notified by CISA Central that the emergency response for the event is at the

[7] The CISA National Infrastructure Simulation and Analysis Center (NISAC) provides advanced modeling and simulation capabilities for the analysis of critical infrastructure vulnerabilities; interdependencies; and the cascading effects of infrastructure loss, damage, or destruction over time. During emerging or actual incidents, the NISAC produces assessments that: 1) Integrate current situation data with pre-established infrastructure modeling, simulation, and analysis; 2) Project consequences of an incident, pre-incident, or post-incident; and 3) Inform response and recovery activities after an incident has occurred. In support of the incident response, the NISAC may conduct updates to existing assessments or perform new assessments to provide the most current situation data to decision-makers.

national level, the Chemical SRMA would notify the Chemical SCC leadership of the need to implement this SOP at the Phase 3 level.

- The Chemical SCC leadership and the Chemical SRMA need to be as proactive and responsive as possible. A false alarm is better than a poor response, especially when lives may be in danger.

Phase 1 — Guarded (72-96 hours prior to event impact)

For severe weather or other advance-notice events, activate Phase 1 Guarded when the weather forecast or other information source identifies an intense or rapidly strengthening low pressure storm system, high pressure storm (i.e., tropical storm/hurricane watch or warning), or like event that has the potential to or is projected to require a coordinated government/SCC response.

During Phase 1, the Chemical SRMA and the Chemical SCC should:

- Establish detailed situational awareness on threats/hazards. By conducting more detailed information gathering, the Chemical SRMA and the Chemical SCC acquire the necessary information to support decision-making and coordination activities in preparation for a transition to incident management activities.
- Review emergency plans and protocols and conduct communications checks.
- Review (and disseminate to Chemical SCC membership, as appropriate) analysis and modeling for hazards, impacts, and interdependencies provided by NISAC, the National Risk Management Center (NRMC), and FEMA, when available.
- Remind Chemical SCC members to update HSIN access information, including user name and password information. In turn, the Chemical SCC should alert its member organizations to do the same.
- Monitor HSIN-CI for situation updates and other relevant information.
- Establish a schedule for conference calls between the Chemical SRMA and the Chemical SCC or provide maximum feasible notice of any unscheduled calls.
- Conduct cross-sector collaboration/communication (including RFIs/RFAs), as appropriate.
- The Chemical SRMA will submit and ensure response to RFIs or RFAs from Chemical Sector stakeholders.
- The Chemical SRMA will create weekly written briefs that will advise SCC of potential "advance notice events" so that they are on the radar to raise awareness and visibility for the sector.

Phase 2 – Concern (48-72 hours prior to event impact)

When CISA makes the decision that the event is still likely to meet a critical threshold, the Chemical SRMA shall notify Chemical SCC leadership of the initiation of Phase 2 additional activities:

- Chemical SCC leadership will notify SCC representatives of the phase level increase from Phase 1 (Guarded) to Phase 2 (Concern).
- Chemical SRMA will contact Chemical SCC leadership to determine if a Chemical Sector-specific teleconference is necessary.
- Chemical SCC representatives will solicit feedback from their respective members regarding preparatory efforts underway in the potential impact zone.
- Chemical SRMA will send an email to the Chemical SCC (and others, as appropriate, such as state chemical councils) inviting SCC organizations and their members to participate in a Chemical

Sector-specific and cross-sector teleconference to discuss the impending threat and determine future actions, if deemed necessary.

- Chemical SRMA will review (and disseminate to Chemical SCC membership, as appropriate) analysis and modeling for hazards, impacts, and interdependencies provided by NISAC, the National Risk Management Center (NRMC), and FEMA, when available (see Appendix J for more information).
- Conduct cross-sector collaboration/communication, as appropriate.
- Chemical SRMA and Chemical SCC will continue to monitor HSIN-CI for situation updates and other relevant information.

Chemical Sector-Specific Conference Call

Timing of Calls – The Chemical SRMA and the Chemical SCC leadership will review the schedule of planning meetings and incident teleconferences scheduled by CISA, available information on the regional incident teleconference, and the time zone of the impact area to determine an appropriate time and frequency for sector-specific teleconferences. The Chemical Sector-specific calls should be scheduled prior to cross-sector calls so that the latest outcomes of the sector-specific call and additional information gathered from sector representatives can be reported out by the Chemical SCC leadership on the cross-sector call.

Topics typically discussed during the sector-specific calls include:

- Impact analysis and modeling from CISA (if available)
- Hazard modeling from FEMA (if available)
- Industry concerns/issues
- Industry RFIs/RFAs
- Location of incident information on HSIN
- How to reset HSIN passwords or request HSIN access
- Timing for the next sector-specific call (see Appendix H for a sector-specific conference call agenda)

Following the sector-specific call, the Chemical SRMA will normally:

- E-mail a short recap of the sector-specific call to the Chemical SCC.
- Send RFIs/RFAs received during sector-specific call to CISA Central/CISA Critical Infrastructure Crisis Action Team (CI-CAT).

Phase 3 – Urgent (less than 48 hours' notice prior to event impact or no warning)

When CISA makes the decision that the event is still likely to meet a critical threshold, the Chemical SRMA shall notify Chemical SCC leadership of the initiation of Phase 3 additional activities:

- Chemical SRMA will coordinate with the Chemical SCC Chair and Vice-Chair, or designee, to assess the need for a sector-specific call and conduct call as determined.
- Chemical SRMA will follow DRAFT agenda for call(s) and conduct post-call activities as described above.
- Chemical SRMA will maintain open communications with the Chemical SCC to ensure they are receiving information and participating in the cross-sector calls initiated by DHS.
- Chemical SRMA will discuss NISAC, NRMC, and/or FEMA Hazards/impacts/interdependencies analysis and modeling with Chemical SCC (if available).

- Discuss Federal Government plume modeling information and related public guidance with Chemical SCC (if applicable).[8]
- Chemical SCC will provide preliminary damage assessment information as soon as practicable to the Chemical SRMA to support national incident reporting (see Appendix E for national incident reporting).
- Chemical SCC and Chemical SRMA will coordinate on cross-sector RFIs/RFAs.
- Chemical SRMA will coordinate with CISA Protective Security Advisors (PSAs) and Chemical Inspectors to assess chemical critical infrastructure owners and operators' needs in the impact area and ascertain emergency shutdown status.
- Chemical SRMA will work with CISA Central to catalog and provide follow-up on all sector RFIs/RFAs.
- Chemical SRMA and Chemical SCC will continue to monitor HSIN-CI for situation updates and other relevant information.

Recovery

Recovery activities take place following the immediate initial response to an event and extend through restoration of key critical infrastructure facilities, functions, systems, services, and supply chains. Termination of recovery-focused coordination and critical infrastructure partner activities will be decided jointly between the Chemical SRMA and the Chemical SCC leadership. The following activities will be conducted during this phase:

- Chemical SCC will provide sector-specific knowledge and expertise to address sector needs and provide government decision-makers and sector partners with the information needed to plan and conduct recovery activities such as, but not limited to:
  - Security needs
  - Safe zones
  - Marshaling areas
  - Escorts (highway)
  - Reentry access
  - Critical needs
    - Electricity
    - Employees within impacted zones, industry, and responders
    - Essentials (food, water, and medical)
    - Emergency housing
    - Communications
    - Fuel[9]
    - Banking and finance

[8] Plume model information includes information resulting from a facility or transportation modality release, or malicious actor use of a weapon of mass destruction impacting the sector.

[9] See Appendix I for information on a comprehensive "checklist" developed by the Oil and Gas Sector Coordinating Council of all Federal regulatory waivers needed to ensure the most efficient functionality of the fuel distribution system possible during a state of emergency (e.g., hurricane, wildfire, blizzard, etc.).

- Chemical SRMA will collect follow-on damage assessment and status reports from the Chemical SCC and evaluate infrastructure restoration priorities (see Appendix D for a list of crisis management status).
- Chemical SRMA will work with sector partners per the NRF to ensure that Chemical Sector infrastructure is recovered in a timely and efficient manner to minimize the impact of service disruptions.
- Sector partners will continue to coordinate, manage, and participate in sector-specific and cross-sector conference calls.
- Sector partners will continue to monitor HSIN-CI for situation updates and other relevant information.
- Chemical SRMA will work with CISA Central to monitor status of outstanding RFIs/RFAs and provide updates to the Chemical SCC, as appropriate.
- Chemical SRMA and Chemical SCC will complete an After-Action Report following real-world incidents and exercises.
- Chemical SCC will coordinate an industry debrief following incidents, as well as following the end of the related hazard season or cycle.

Cross-Sector Resilience Practices

It is pertinent that critical infrastructure sector stakeholders collaborate during all stages of an incident to create a common operating picture throughout the response and recovery process. Within emergency response protocols, the Chemical Sector must focus on coordination and communication between private and public sector stakeholders. This is important to determine which trigger points require response activation and to effectively examine long term recovery operations and interdependencies related to supply chain impacts across multiple critical infrastructure sectors.

To effectively support incident management and coordination, the Chemical SCC and SRMA must be prepared to collaborate with other critical infrastructure sectors SRMAs and SCCs/GCCs to secure the nation's critical infrastructure. This is vital to proper emergency management because most individual sectors have well-established protocols for preparing for and responding to a severe incident, however, there does not seem to be extensive knowledge of how other sectors would respond. It is beneficial to bring together representatives from each sector at all stages of an incident to allow for cross-sector collaboration that can better address individual sector needs.

- **Preparedness**: Private and public sector partners must recognize the value of playbook coordination between various critical infrastructure sectors to ensure synchronized information sharing, response, and recovery efforts in the event of an emergency incident. The Chemical Sector and other Critical Infrastructure partners must coordinate individual sector playbooks in support of cross-sector incident response planning.
- **Pre-Incident**:
    - *Water Sector:* Water sector representatives would coordinate pre-incident operations with federal partners to include the Environmental Protection Agency (EPA), Federal Emergency Management Agency (FEMA), and subject matter experts (SMEs) to establish contact with affected regions and provide recommendations for mitigating impacts to utilities and other essential public services.

    - *Chemical Sector:* The Chemical sector would engage in pre-incident conference calls with the Chemical Sector SRMA and SCC to determine how to respond to RFIs and RFAs from private sector partners.
    - *Energy-Electricity Sub-Sector:* The Electricity SCC would conduct a senior management-level call to ensure public and private sector coordination pre-response and coordinate mutual assistance through a national response framework. The Electricity subsector also has a tri-sector playbook with the Communications and Finance sectors to ensure consistent and unified messaging in the wake of post-incident outages.
    - *All Sectors:* Sectors can use resources such as the National Business Emergency Operations Center (NBEOC) for a cross-sector view of incident-related information gathering and sharing. However, it is important to note that the information provided is often generalized rather than sector specific. Thus, the chemical sector makes a commitment to assist with establishing smaller sector-level discussions to triage NBEOC information and identify sector-specific needs leading up to a severe incident. The Chemical SCC and other private sector stakeholders have well-established relationships with federal entities in their respective sectors, but there is currently no formal process for coordination with state and local partners, including federal partners at the state and regional levels. Regional entities can quickly address RFIs and identify regional and federal-level assistance available to private sector partners, including mutual aid, inventory sharing, and other resources. In most cases, the regional entities can help quickly identify friction points where federal government partners can streamline the process and expedite resource requests.

Preparedness Questions Answered:

- What would your sector be doing pre-incident to adequately prepare?
    - How would the sector's posture change during the incident, and post-incident?
- What systems are available that can facilitate information sharing and coordination among all stakeholders and sectors? Are redundancies built into your communication plans?

Preparedness Questions Still to Address:

- What information does your organization need to trigger and implement playbooks or supply chain continuity plans?
- What information would your sector expect or need from another sector at this point?
    - What would constitute a critical point(s) for information sharing to begin among sectors?
- What would be the trigger for a multi-sector stakeholder telephone conference?
- Does your organization have any obligations that will not be fulfilled because of a disruption to your supply chain?
- What considerations regarding re-entry are being made at this time for each sector?

Overall, the Chemical Sector needs to collaborate with other critical infrastructure sectors to determine what are proper and relevant coordination efforts for response and recovery during and after an incident.

SECTION 5: SOP MANAGEMENT AND MAINTENANCE

The Chemical SCC will coordinate with the Chemical SRMA on the update, revision, maintenance, and distribution of this SOP. This SOP will be reviewed on an annual basis during the first quarter of each year, at a minimum, so it remains current and compliant with policy, process, and protocol changes. In addition, the Chemical SRMA and the Chemical SCC will complete an after-action report following real-world incidents and exercises involving the Chemical Sector to ensure that the SOP is updated to reflect identified best practices, lessons learned, and areas for improvement. Proposed continuity of operations changes or revisions to the SOP will be jointly reviewed and approved by the Chemical SRMA and the Chemical SCC. Copies of the revised SOP will be distributed to the Chemical SCC membership. The Chemical SRMA will maintain the official copy of the approved SOP.

APPENDIX A: EMERGENCY CONTACT LISTS

It is important to identify response agencies and stakeholders in your community and geographic region and to build relationships with these groups before an incident occurs.

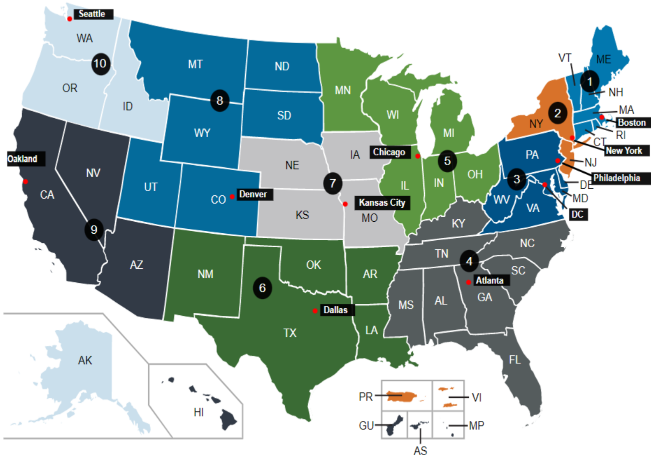
Resource	Contact	Phone Number
Facility Security Officer		
Facility Safety Officer		
Facility Information Technology Manager		
Chief of Regulatory Compliance (if applicable)		
City Law Enforcement		
County Law Enforcement		
State Law Enforcement		
Local Fire Service		
City Emergency Management		
County Emergency Management		
State Emergency Management		
Federal Bureau of Investigation (FBI) local Field Office	www.fbi.gov/contact-us/field-offices	Varies
FBI Weapons of Mass Destruction (WMD) Coordinator at local FBI office	FBI Headquarters — FBI	N/A
CISA Protective Security Adviser (PSA) for this state/district	PSCDOperations@hq.dhs.gov	703-235-9349
DOT Emergency Preparedness, Response and Recovery Website	www.dot.gov/emergency	N/A
DHS Chemical Facility Anti-Terrorism Standards (CFATS) Tip Line	CFATSTips@hq.dhs.gov	877-394-4347
CFATS Helpdesk	CFATS@hq.dhs.gov	866-323-2957
CISA Central	central@cisa.dhs.gov	888-282-0870
Chemical Sector Management Team	ChemicalSector@cisa.dhs.gov	202-322-6974
DHS Chemical Security Analysis Center (CSAC)	csac.reachback@hq.dhs.gov	410-417-0910
DHS Priority Telecommunications Service Center	support@priority-info.com	866-627-2255
U.S. Coast Guard National Response Center (if applicable)	www.nrc.uscg.mil	800-424-8802
HSIN Password Reset	HSIN.helpdesk@hq.dhs.gov	866-430-0162

Incident Management Communication

Sector Coordinating Council		SRMA Management Team
SCC Chair: Gary Davis Director of Security Air Liquide Gary.davis@airliquide.com Mobile: 713-259-4803	**SCC Vice Chair: Carey Waltz** Head of Group Security, NA Linde PLC Carey.Waltz@Linde.com Mobile: 520-990-0206	**Jacob Mehl** Stakeholder Engagement Division, Chemical Sector Management Team Section Chief Jacob.Mehl@cisa.dhs.gov ChemicalSector@cisa.dhs.gov Mobile: 202-322-6974
SCC Asst. Vice Chair: Robyn Brooks Vice President - Health, Environment, Safety and Security The Chlorine Institute robyn.brooks@cl2.com Mobile: 703-894-4115	**SCC Asst. Vice Chair: Trevor Hampton** SCC Assistant Vice Chair Manager, Chemical Security Trevor_Hampton@americanchemistry.com Mobile: 540-379-5645	

Regional Office Locations and Contact Information

Region	Regional Director			
	Name	Phone Number	Email Address*	Operations Email**
1	Matt McCann	(617) 840-5469	CISARegion1@hq.dhs.gov	CISA.IOD.Region.R01._OPS.MB@cisa.dhs.gov
2	John Durkin	(646) 235-7808	CISARegion2@hq.dhs.gov	CISA.IOD.Region.R02._OPS.MB@cisa.dhs.gov
3	Bill Ryan	(215) 292-9134	CISARegion3@hq.dhs.gov	CISA.IOD.Region.R03._OPS.MB@cisa.dhs.gov
4	Dr. Joy Purser	(904) 254-0465	CISARegion4@hq.dhs.gov	CISA.IOD.Region.R04._OPS.MB@cisa.dhs.gov
5	Alex Joves	(312) 350-7794	CISARegion5@hq.dhs.gov	CISA.IOD.Region.R05._OPS.MB@cisa.dhs.gov
6	Harvey Perriott	(214) 702-0294	CISARegion6@hq.dhs.gov	CISA.IOD.Region.R06._OPS.MB@cisa.dhs.gov
7	Phil Kirk	(913) 498-3786	CISARegion7@hq.dhs.gov	CISA.IOD.Region.R07._OPS.MB@cisa.dhs.gov
8	Shawn Graff	(720) 660-3201	CISARegion8@hq.dhs.gov	CISA.IOD.Region.R08._OPS.MB@cisa.dhs.gov
9	David Rosado	(916)-304-4773	CISARegion9@cisa.dhs.gov	CISA.IOD.Region.R09._OPS.MB@cisa.dhs.gov
10	Patrick Massey	(206) 384-0750	CISARegion10@hq.dhs.gov	CISA.IOD.Region.R010._OPS.MB@cisa.dhs.gov



*For steady-state, non-emergency situations, contact the regional office via the regional email address.

**During incidents, contact the regional office via the regional incident operations team email address. *Note: these distribution lists are not accessible outside DHS.*

Across the nation, CISA’s Regional Offices offer a range of cyber and physical services to support the security and resilience of critical infrastructure owners and operators and state, local, tribal, and territorial partners. Protective Security Advisors (PSAs), Chemical Security Inspectors (CSIs), Cyber Security Advisors (CSAs), Emergency Communications Coordinators, and visiting CISA headquarters staff all coordinate their critical infrastructure protection missions through the regional offices, and collaborate on regional critical infrastructure efforts, as needed.

State Chemical Association Contact Information

LAST NAME	ORGANIZATION	ADDRESS	CITY	STATE	ZIP CODE	PHONE	EMAIL
Barganier	Manufacture Alabama	401 Adams Avenue Suite 710	Montgomery	AL	36104	(334) 386-3000	jon@manufacturealabama.org
Clark	Manufacture Alabama	401 Adams Avenue Suite 710	Montgomery	AL	36104	(334) 386-3000	george@manufacturealabama.org
Johnson	Chemical Industry Council of California	2420 Sand Creek Road C1 #259	Brentwood	CA	94513	(925) 308-4601	llwjohnson@comcast.net
Bowen	Manufacturers Association of Florida	1625 Summit Lake Drive Suite 300	Tallahassee	FL	32317	(850) 402-2954	Abowen@mafmfg.com
Biel	Chemical Industry Council of Illinois	400 W. Monroe Street Suite 205	Springfield	IL	62704	(217) 522-5805	mbiel@cicil.net
Cress	Kentucky Chemical Industry Council	609 Chamberlin Avenue	Frankfort	KY	40601-4220	(502) 3524612	rcress@dinsmore.com
Bowser	Louisiana Chemical Association	One American Place Suite 2040	Baton Rouge	LA	70825	(225) 344-2609	greg@lca.org
Robertson	Massachusetts Chemistry Technology Alliance	37 Dawson Road	Worcester	MA	01602-1212	(508) 791-0445	katherine@masscta.org
Dulmes	Michigan Chemistry Council	2501 Jolly Road Suite 110	Okemos	MI	48864	(517) 372-8898	john@michiganchemistry.com
McKay	Mississippi Manufacturers Association	720 N President St	Jackson	MS	39202	(601) 292-1119	Johnm@mma-web.org
Hart	Chemistry Council of New Jersey	Capitol View Building 150 West State Street	Trenton	NJ	08608	(609) 392-4214	Dhart@chemistrycouncilnj.org
Howard	North Carolina Manufacturers Alliance	620 N. West Street Suite 101	Raleigh	NC	27603	(919) 834-9459	preston.howard@myncma.org
Klein	Ohio Chemistry Technology Council	88 East Broad Street Suite 1490	Columbus	OH	43215-3535	(614) 224-1730	Jklein@ohiochemistry.org
Foster	Pennsylvania Chemical Industry Council	200 N. 3rd Street Floor 10	Harrisburg	PA	17101-1587	(717) 214-2200	foster@pcic.org
Hazzard	South Carolina Chemistry Council, South Carolina Manufacturers Alliance	1340 Bull Street	Columbus	SC	29201-3475	(803) 799-9695	Sara@myscma.com
Jackson	Tennessee Chamber of Commerce and Industry	414 Union Street Suite 107	Nashville	TN	37219-1724	(615) 256-5141	bradley.jackson@tnchamber.org
Rivero	Texas Chemical Council	1402 Nueces Street	Austin	TX	78701-1508	(512) 646-6401	Rivero@texaschemistry.org
Vassey	Virginia Manufacturers Association	2108 West Laburnum Avenue	Richmond	VA	23227	(804) 643-7489	bvassey@vamanufacturers.com
Randolph	West Virginia Manufacturers Association	2001 Quarrier Street	Charleston	WV	25311-2212	(304) 342-2123	rebecca@WVMA.com

APPENDIX B: CHEMICAL SECTOR OWNER/OPERATOR AND STATE, LOCAL, TRIBAL, AND TERRITORIAL AGENCY RESPONSIBILITIES

For purposes of this SOP, Chemical Sector owners/operators and SLTT agencies have the following general responsibilities regarding incident management.

Chemical Sector Owners/Operators

- Direct local facilities to coordinate with SLTT authorities on preparedness and response activities and RFIs/RFAs.
- Inform respective Chemical SCC associations/organizations of preparedness and response activities, incident impacts, and RFIs/RFAs to allow the Chemical SCC and Chemical SRMA to work collaboratively to monitor and ensure that RFIs/RFAs are captured in national incident reporting mechanisms and implementation tracking system overseen by the CISA Central.

State, Local, Tribal, Territorial, and Insular Area Agencies

- Establish security and resilience partnerships, facilitate information sharing, and enable planning for critical infrastructure protection within their jurisdictions.
- Develop and implement statewide, local area, or regional critical infrastructure protection programs integrated into homeland security and incident management programs.
- Serve as crucial coordination hubs, bringing together prevention, protection, response, and recovery authorities, capacities, and resources among constituent jurisdictions, across sectors, and across regional entities.
- Act as conduits for RFAs when the threat or incident situation exceeds the capabilities of public and private sector partners in their jurisdictions.
- SLTT governments usually are responsible for emergency services and first-level responses to incidents.
- In some critical infrastructure sectors SLTT governments own and operate critical infrastructure, such as water, wastewater, and storm water systems and electric utilities, and are responsible for initial prevention, response, recovery, and emergency services provision.

APPENDIX C: CISA CENTRAL REQUEST FOR INFORMATION/ ASSISTANCE

RFI/RFAs are submitted to the central inbox via central@cisa.dhs.gov and CISA Central fields all requests that are received. There is no specific form to be completed at this time.

For more information regarding CISA Central RFI/RFA process, contact CISA Central at central@cisa.dhs.gov or call 202-282-9201.

APPENDIX D: CRISIS MANAGEMENT STATUS REPORT FOR CHEMICAL SECTOR

Business/Association:

Key Contact:

No Issues – Operational

Impacted
Number of Sites:

- **Physical**
    - Shutdown
    - Out-of-Service
    - Fire
    - Flood
    - Destroyed
    - Product release with significant or potentially significant environmental or human impacts
    - Spills with significant or potentially significant environmental or human impacts
- **Infrastructure**
    - Communication
        - Phone
        - Cyber
    - Electric
    - Gas
    - Highway
    - Rail
    - Port
- **Employee**
    - No Impact
    - Impacted
        - Unknown Status
        - Missing
- **What are the immediate needs?**
    - Support
    - Information
        - Agency Contacts
        - Aerial Photos

Response

- **Return to Work – Access Control**
- **Government**
    - Exemptions
    - Highway
    - Rail
    - Fuel
    - Escorts
- **Additional Security**
    - Contractor
    - Local Law Enforcement Officer
    - State/National Guard

APPENDIX E: CISA INCIDENT RESPONSE PLAN

When directed by CISA Central, the Chemical SRMA must provide information on impacts to the sector from an incident to CISA Central and the CISA Crisis Action Team. Information gathered is used by CISA Central to prepare situation reports which are provided to senior levels in government, SCCs, and owners/operators via HSIN.

Information that must be provided under a data call includes:

- Impacts to national and/or regional critical infrastructure within the incident area
- Restoration Activities
- Key Current Actions (previous 24-48 hours)
- Key Future Actions (next 24-48 hours)
- Federal Resource Commitment (available/committed/requested/received)
- Loss or Degradation of Key Capabilities

APPENDIX F: HOMELAND SECURITY INFORMATION NETWORK – CRITICAL INFRASTRUCTURE (HSIN-CI) INFORMATION

Homeland Security Information Network–Critical Infrastructure

The Homeland Security Information Network–Critical Infrastructure (HSIN-CI) is a national, secure, trusted Web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.

HSIN is a network of "Communities of Interest," which are organized by state organizations, federal organizations, or functional areas, such as emergency management, law enforcement, critical sectors, and intelligence. Users can securely share within their communities or reach out to other communities as needed. HSIN provides secure, real-time collaboration tools, including a virtual meeting space, instant messaging, and document sharing. HSIN also allows partners to work together instantly, regardless of their location, to communicate, collaborate, and coordinate.

The Community of Interest for the Critical Sectors is HSIN-CI. Within HSIN-CI, there are subportals available for each sector, with the subportal for the Chemical Sector referred to as HSIN-CI Chemical Sector. CISA Central posts threat products, suspicious activity information, and incident information on HSIN-CI. The Chemical SRMA posts information specific to the Chemical Sector on HSIN-CI.

Joining HSIN

Membership in HSIN is based on Community of Interest. Owners and operators of chemical manufacturing, storage, and transportation facilities, as well as Chemical SCC members, are eligible for access to HSIN-CI Chemical Sector. If you work in another critical infrastructure sector, visit the Critical Infrastructure Sectors Page to determine the most appropriate HSIN-CI site for you.

If you need more information, contact the HSIN Outreach Team e-mail at HSIN.Outreach@hq.dhs.gov.

To request access to HSIN-CI, submit the following to HSINCI@hq.dhs.gov:

- Name
- Employer
- Title
- Business email
- Brief written justification

Once nominated, the Community of Interest Validating Authority will review your membership application and approve or deny your admission to the Community of Interest. If the application is approved, an e-mail will be sent to you with instructions on how to log onto HSIN for the first time.

Although passwords can be reset online, current users can also request password help and other assistance on HSIN use by contacting the HSIN Help desk at 1-866-430-0162 or HSIN.helpdesk@hq.dhs.gov.

APPENDIX G: INDUSTRY/ASSOCIATIONS PREPAREDNESS CHECKLIST

Status Reporting

- Status Updates
- Impact Zone (ground zero & surround)
- General Overview (impacted area and specific sectors)

Critical Infrastructure or Support Zones

- Forecast
- Operational Status
- Employee Status (based on day & time)
- Time & Repeat Schedule (impact based)

Establish Primary Points of Contact (POCs)

- Government
- State
- Fusion Centers (Emergency Ops Center)
- Government Agencies
- Sector Contacts
- Impacted Industry(as warranted)

Chemical Sector Response

- Underway
- Scheduled
- Planned

Response Update

- Industry
- Government
- Security
- Safe Zones
- Marshaling Areas (response)
- Escorts (highway)

Critical Needs

- Credentialed Employees, Industry, and First Responders (within impact zones)
- Essentials (food, water, and medical)
- Emergency Housing
- Communications
- Fuel
- Banking

Status Update

- Responding and Start-ups
- Time and Schedule (based on impact)
- Impacted Zones (ground zero and surrounding area)

Regulatory Relief

- Permits, Exemptions, etc.
- Status
- How to Request

Reentry

- States/Local (Parish) data – review
- Business

APPENDIX H: DRAFT AGENDA FOR CHEMICAL SECTOR-SPECIFIC CALLS

Call Meeting to Order

- SRMA provides short status recap (from current incident situation reports provided by CISA Central)
- Usually focused on power restoration, transportation, and port status

Impact Zone (Forecasted)

- General overview of impacted area and specific sectors
- Critical infrastructure or support zones
- Pre-planning – evacuations

Industry Activity

- Determine what actions, in general, industry is taking
- If any facility operator thinks they are a sole producer and their facility is down, ask them to contact the SRMA separately
- Try to determine if the facility is a sole provider and evaluate cascading impacts

Reentry

- States/Local (Parish) data – review
- Business Continuity

Primary POC (Point of Contact) and Activation Status

- Emergency Operations Centers
- Fusion Centers
- SLTT Government Agencies
- Federal Joint Field Office
- Sector Contacts
- CISA Protective Security Advisors

Planning

- Develop a schedule and a hand-off process

APPENDIX I: REGULATORY RELIEF TO FACILITATE MOVEMENT OF SUPPLIES DURING AN EMERGENCY

The chemical industry operates under a myriad of regulations that dictate product quality and contribute to safe operations and environmental performance. The industry has a deep commitment to complying with all regulations, all of the time—this includes during emergency situations. The industry bears the responsibility for delivering chemicals to consumers and is adept at adjusting supply chains within the limits of applicable regulations to overcome day-to-day operational issues or issues that arise from natural disasters. Temporary relaxation of certain regulatory requirements can allow for expedited response and recovery from natural disasters. Prudently issued regulatory relief that appropriately balances competing concerns allows the government to temporarily suspend certain regulatory requirements so that companies can accelerate recovery to help alleviate the emergency and restore normal operating conditions to best serve the public interest.

This section includes a list of possible regulatory waivers that may be necessary during a state of emergency to help expedite recovery and explanations of when regulatory relief may be appropriate. Further information on regulatory relief can be found in the recent National Petroleum Council study on "Enhancing Emergency Preparedness for Natural Disasters"

Environmental Protection Agency (EPA)

1. **RFG Requirements**

   Issue: Reformulated gasoline (RFG) is a cleaner burning gasoline blend required in areas that are not meeting certain air quality standards. During times of emergency, it is imperative that distributors have the flexibility to get any available fuel into the affected area in any way possible, regardless of whether it is RFG.

   Waiver Needed: 40 CFR 80.78(a)(7), which prohibits persons from combining any reformulated gasoline blendstock for oxygenate blending with any other gasoline, blendstock, or oxygenate.

2. **ULSD Requirements**

   Issue: Ultra Low Sulfur Diesel (ULSD) is a cleaner fuel, with a 15 parts per million (ppm) sulfur specification, required by EPA for vehicles and equipment. During times of emergency, it is imperative that distributors have the flexibility to get any available fuel into the affected area in any way possible, regardless of the sulfur content.

   Waiver Needed: 40 CFR 80.510 and 80.520, which sets ULSD standards. This waiver would allow the use of high sulfur heating oil in model year 2006 and older vehicles, generators, and as home heating oil during the emergency.

3. **Vapor Recovery Regulations**

   Issue: Fuel terminal loading and unloading systems and tank trucks that transport fuels are required to use specified vapor recovery equipment, which can differ from state to state. In the case of an emergency, it is imperative that fuel can move from jurisdiction to jurisdiction by any transport means available. The states include these regulations in their state implementations plans (SIPs) which are approved and enforced by the EPA.

   Waiver Needed: 40 CFR Part 60 Subpart XX and Part 63 Subparts R, Y, and BBBBBB, which set the standards for loading applicable to bulk gasoline terminals, pipeline breakout stations, and marine tank vessel loading operations, respectively.

Department of Transportation (DOT)

To expedite oversize/overweight permitting and to assist with toll information, waivers and other transportation related issues, DOT developed a department wide DOT Emergency Preparedness, Response, and Recovery Information Website (www.dot.gov/emergency). During an emergency DOT will post information related to transportation permits, waivers, and other regulations and authorities that are applicable during an emergency to assist all public and private transportation organizations. The website contains links to each of the DOT Operating Administration's emergency websites and the Emergency Support Function – 1 (Transportation) Partner agencies.

For road closures, DOT will provide FEMA major interstate and other significant road closures, however FEMA and the private sector should access the state DOT 511 Websites (which are linked from DOT's emergency website) to obtain this information.

1. **General Administrative Requirements**

   Issue: DOT's Federal Motor Carrier Safety Administration (FMCSA) sets general standards and requirements that apply to vehicle labeling and record keeping, among others. They also require transporters to follow all applicable state and federal requirements. This section needs to be waived in order to expedite shipments of fuel to recovery areas and to allow for other federal and state waivers to be effective.

   Waiver Required: 49 CFR 390, which provides the general basis for federal motor carrier safety regulations.

2. **Driver Qualification Regulations**

   Issue: FMCSA has certain rules, such as requiring a driver's physical fitness, fluency in the English language, level of fatigue, the thorough inspection of cargo, lighting and cargo standards, and inspection repair and maintenance, that may be appropriate under regular operating circumstances, but hinder the effort to get as many loads into the disaster area as possible in a short amount of time.

   Waiver Required: 49 CFR Parts 391-3 and 396, which set driver standards, load standards, inspection standards, etc.

3. **Hours of Service Regulations**

   Issue: FMCSA sets requirements on how many hours a truck driver can drive or be on duty in a given day and week. There are also certain rest time requirements between on-duty periods. These requirements, which may be appropriate under regular operating circumstances, hinder the effort to get as many loads into the disaster area as possible in a short amount of time.

   Waiver Required: 49 CFR Part 395, which sets hours of service regulations.

4. **Vehicles Not Meeting HazMat Specifications**

   Issue: DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA) sets strict specifications on which and how vehicles can carry gasoline and other hazardous materials and (i.e., shipping papers, markings, placarding, etc.). To get the needed quantities of fuel into the disaster area as quickly as possible, more vehicles are needed as long as they are fit to carry gasoline and diesel fuel, even if they do not meet the strict specifications.

   Waivers Required: 49 CFR Parts 173.242 and 172 Subparts C, D, F, and I, which govern vehicle specifications and other shipping standards for tank trucks. These waivers will also affect 49 CFR Parts 106, 107, and 171-180.

5. **Jones Act**

   Issue: The Merchant Marine Act, also called the Jones Act, requires that only U.S. built and flagged vessels can carry goods from U.S. ports to other U.S. ports. During times of emergency it is imperative that disaster relief items, including fuel, get to the disaster area as quickly as possible regardless of country of origin. More eligible vessels mean that more disaster relief supplies arrive in a timelier fashion. Coastwise waivers can be granted in two ways: (1) waivers shall be granted automatically on request of the Secretary of Defense to the extent considered necessary in the interest of national defense to address an immediate adverse effect on military operations; and (2) when the "head of an agency responsible for the administration of the navigation or vessel-inspection laws" (in this case the Secretary of DHS) considers it necessary in the interest of national defense, if the Administrator of MARAD determines that no U.S.-flagged vessels are available for the proposed transportation. CBP has direct responsibility for enforcing the Jones Act and processes requests for waivers for the Secretary of DHS. Prior to granting the waiver, CBP must seek MARAD's advice regarding U.S.-flag vessel availability before the Secretary of DHS makes a decision by law (see 46 U.S.C. § 501).

   Waiver Required: 46 USC 551, which codifies the restriction on non-U.S. flagged vessels delivering from U.S. ports to U.S. ports.

Internal Revenue Service (IRS)

1. **Diesel Fuel Penalty**

   Issue: The IRS imposes 24.4 cents per gallon tax on diesel fuel sold for on-road use, while dyed diesel fuel, used for farming purposes, home heating use, etc., is not ordinarily subject to the tax. Typically, if a diesel fuel that was not subject to this excise tax was converted to use for on-road purposes, the IRS would require that use to be reported and the tax paid accordingly. In the case of emergency, the goal is to get as much transportation fuel into the market as possible to make up for supply shortages, and, as such, this reporting and tax requirement becomes an impediment to bringing that fuel into the transportation mix.

   Waiver Required: Requirements under Publication 510 of the Internal Revenue Code, which governs excise taxes.

Other Federal Government Assistance

1. **Coast Guard: Vessel Movement Control**

   Issue: The Coast Guard has authority to control vessel traffic in areas subject to the jurisdiction of the United States that are determined to be hazardous or under other hazardous circumstances through enactment of safety and security zones. Coordination efforts with the U.S. Coast Guard to provide exclusive access to ports in the disaster area to those bringing fuel and other necessary supplies to expedite barge movement is necessary.

   Waiver Required: Captain of the Port Order waiver under Ports and Waterways Safety Act (33 USC 1221 et. seq.).

2. **DOD/DHS: Fuel Loans and Distribution Assistance –** Assistance can be obtained through the Department of Defense's Defense Logistics Agency and the Federal Emergency Management Administration.

3. **DOE: Fuel Loans –** Coordinate with the U.S. Department of Energy.

State Waivers that may be necessary to Transport Fuel/Chemicals Interstate

1. **Reid Vapor Pressure (RVP) Requirements**

   Issue: Many states allow a variance, up to 1 lb. RVP, from the most recent version of ASTM D4814 for gasoline blended with ethanol. NIST Handbook 130 also provides for this variance.

   Waiver Required: States that do not allow for an RVP variance should waive the applicable state law or regulation to allow fuel from states that do allow the variance to be used interchangeably across state lines during the emergency.

2. **Biofuel Blending Requirements**

   Issue: Some states require a minimum amount of biofuels to be blended into all gasoline and/or diesel sold within the state.

   Waiver Required: States with minimum biofuel blending requirements should waive the applicable law or regulation to allow fuel that does not contain the specified volume of biofuels to be carried across state lines and sold in the state during the emergency.

3. **State I Vapor Recovery Requirements**

   Issue: Fuel terminal loading and unloading systems and tank trucks that transport fuels are required to use specified vapor recovery equipment, which can differ from state to state. In the case of emergency, it is imperative that fuel can get from jurisdiction to jurisdiction by any transport means available. The states include these regulations in their state implementations plans (SIPs), which are approved and enforced by EPA.

   Waiver Required: During an emergency, if EPA provides a waiver (or no action assurance) during the emergency, each state requiring Stage I Vapor Recovery should waive the applicable law or regulation to allow trucks and terminals without vapor recovery equipment to operate and move fuel from the terminal to intrastate or interstate destinations.

4. **Weight Limits**

   Issue: All states set weight restrictions (maximum weights allowable) for trucks that travel on their roadways. Because federal law allows each state to set their own weight requirements, not all states set the limits at the same weight. In addition, these state-specific weight limits typically require fuel tankers to be filled at levels below their capacity in most, if not all, states.

   Waiver Required: States should waive their typical weight limits and set temporary limits for trucks carrying emergency relief supplies (including fuel) to allow rapid movement of the greatest amount of fuel that can be moved safely intrastate and across state lines. A typical waiver may allow transport of 92,000 lbs. to 100,000 lbs.

5. **Distributor License**

   Issue: Many states require a carrier to pay a fee and obtain a Distributor's License to transport motor fuel within the state.

   Waiver Required: States should waive the applicable fees and license requirements to ensure that all drivers, trucks, and resources within the state or brought across state lines to provide support are available to contribute to the disaster relief effort.

6. **Hours of Service**

   Issue: Some states have driver hours-of-service requirements that are more restrictive than DOT regulations.

   Waiver Required: States with hours-of-service regulations that are more restrictive than the federal government should waive those requirements in support of DOT's effort to deliver as many loads into the disaster area as possible in the shortest period of time.

7. **Retail Gasoline Label Requirements**

   Issue: States that have specific biofuel blending requirements may require labels that say things like "contains 10% ethanol," while some fuel transported interstate may not have exactly 10 percent, but rather "up to 10% ethanol."

   Waiver Required: States with content specific labeling requirements should waive those requirements to allow fuels that may not be blended with the exact volume depicted on the dispenser to be sold in the state during the emergency.

8. **Importer/Exporter Licenses**

   Issue: State revenue departments require fuel importers and exporters to pay a fee and obtain a license from the state to move fuel across state lines. Without these licenses, the fuel merchant cannot legally buy gasoline from one state and move it to another.

   Waiver Required: Each individual state within the disaster region should allow fuel to be bought and sold within or outside their state by any merchant, whether or not they have paid the proper fee and obtained an importer/exporter license. For example, states who have allowed a waiver in the past have taken different approaches: some expedite licenses during the emergency, while others waive the requirements entirely or require the merchant to remit taxes to the state despite not being properly licensed and registered.

9. **IRP/IFTA**

   Issue: The International Registration Plan (IRP) is an agreement among the states of the U.S., the District of Columbia, and provinces of Canada providing for payment of commercial motor carrier registration fees. To operate in multiple states or provinces, motor carriers must register in their base jurisdiction (state or province). The International Fuel Tax Agreement (IFTA) is an agreement among states to report fuel taxes by interstate motor carriers.

   Waiver Required: These tax structures, which act as interstate fuel taxes, should be waived in agreement with all states that are affected by the emergency or that are participating in the emergency relief effort to ensure that fuel can move freely from one state to another without the time-consuming tax bureaucracy process.

10. **Anti-Price Gouging Requirements**

    Issue: Most states have regulations which prohibit retail gasoline stations from raising their prices more than a certain amount during a specified time period. While this is intended to protect the consumer, during a supply disruption it has the unintended effect of discouraging gasoline stations from engaging in extraordinary measures to acquire new inventory. Thus, shortages proliferate, and those who genuinely need fuel, and are willing to pay a premium, are unable to obtain it.

    Waiver Required: These market constricting regulations should be waived or modified in order to ensure that retail stations are not discouraged from bringing in fuel from other states or regions due to the inability to earn reasonable profit and recover legitimate costs in doing so.

APPENDIX J: KEY REFERENCES

Chemical Sector Coordinating Council (SCC)

The Chemical Sector Coordinating Council (SCC) is one of 16 critical infrastructure councils established under the protection afforded by the Critical Infrastructure Partnership Advisory Council. The National Plan sector partnership model encourages critical infrastructure owners and operators to create or identify a Sector Coordinating Council (SCC) as the principal entity for coordinating with government at various levels on a wide range of critical infrastructure-related activities and issues. The SCCs are self-organized, self-run, and self-governed to include a spokesperson designated by the sector membership. Specific membership varies from sector to sector, reflecting the unique composition of each sector. However, membership generally is representative of a broad base of owners, operators, associations, and other entities—both large and small—within a sector.

Chemical Sector Government Coordinating Council (GCC)

Formed as the government counterpart to each SCC to enable interagency and cross-jurisdictional coordination, the GCC comprises representatives from across various levels of government (federal, state, local, and tribal), as appropriate to the operating landscape of each individual sector. Each GCC is co-chaired by a representative from the designated SRMA with responsibility for ensuring appropriate representation on the GCC and providing cross-sector coordination with state, local, tribal, and territorial governments. The GCC coordinates strategies, activities, policy, and communications across governmental entities within each sector.

CISA Central

CISA Central is CISA's hub for staying on top of threats and emerging risks to our nation's critical infrastructure, whether they're of cyber, communications or physical origin. CISA Central is the simplest, most centralized way for critical infrastructure partners and stakeholders to engage with CISA and is the easiest way for all critical infrastructure stakeholders to request assistance and get the information you need to understand the constantly evolving risk landscape.

Through CISA Central, CISA coordinates situational awareness and response to national cyber, communications, and physical incidents. CISA works closely with public, private sector, and international partners, offering technical assistance, information security and education to protect our nation's critical infrastructure from a broad range of current cyber, communication, and physical threats. For more information, email Central@cisa.gov. To report a cyber incident, visit www.us-cert.gov/report.

Critical Infrastructure and Key Resources (CIKR) Support Annex to the NRF

The CIKR annex to the NRF describes policies, roles and responsibilities and provides the concept of operations for assessing, prioritizing, protecting, and restoring critical infrastructure within the United States, its territories, and possessions during actual or potential domestic incidents. The annex details the processes to ensure coordination and integration of critical infrastructure-related activities among a wide array of public and private incident managers and security partners within immediate incident areas, as well as at the regional and national levels.

Government Emergency Telecommunications Service (GETS)

A National Communications System (NCS) program, GETS enables users to prioritize calls over wireline networks through an access card (GETS card) that provides both a universal GETS access number and a

Personal Identification Number (PIN) for critical personnel's use during significant incidents. For assistance setting up accounts contact DHS Priority Telecommunications Service Center 1-866-627-2255 or 1-703-676-2255.

Homeland Security Information Network – Critical Infrastructure (HSIN-CI)

HSIN is a national, secure, and trusted web-based portal for information sharing and collaboration between federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission. HSIN consists of a growing network of communities called "Communities of Interest," which are organized by state organizations, federal organizations, or mission areas, such as emergency management, law enforcement, critical sectors, intelligence, etc. The portal provides users the ability to securely share information within their communities or reach out to other communities as needed. HSIN provides threat and incident information and secure, real-time collaboration tools to include a virtual meeting space, instant messaging and document sharing. HSIN-CI also allows partners to work together instantly, regardless of their location, to communicate, collaborate, and coordinate. See Appendix F for HSIN-CI access and additional related information.

National Business Emergency Operations Center (NBEOC)

The NBEOC is FEMA's virtual clearing house to enhance information sharing between private industry partners and public agencies — including FEMA — before, during, and after disasters. When there is an active disaster response, NBEOC members have unique lines of communication into FEMA's National Response Coordination Center, activated Regional Response Coordination Centers, and the broader network of emergency management operations, including state and federal partners. The NBEOC allows members to share knowledge from the field impacting operating status and recovery challenges. It also provides data to help with business continuity decisions, and provides integration into disaster planning, training, and exercises.

National Disaster Recovery Framework (NDRF)

A framework describing the concepts and principles that promote effective federal recovery assistance, the NDRF identifies scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities. It also links federal, state, local, and tribal governments; the private sector; and nongovernmental and community organizations that play vital roles in recovery.

National Incident Management System (NIMS)

NIMS is a framework that provides a systematic, proactive approach to guide departments and agencies at all levels of government, nongovernmental organizations, and the private sector to work seamlessly to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity, in order to reduce the loss of life, property, and harm to the environment. NIMS works hand-in-hand with the NRF. The NIMS provides the template for the management of incidents, while the NRF provides the structure and mechanisms for national-level policy for incident management.

National Infrastructure Protection Plan (National Plan)

The National Plan establishes the overall risk-based construct that defines the unified approach to protecting the nation's critical infrastructure in an all-hazards context and specifies procedures and activities to reduce risk to the nation's critical infrastructure, including:

- The risk management framework used to implement National Plan steady-state protection efforts and provide the critical infrastructure restoration dimension for incident management activities under the NRF.
- The sector partnership model that encourages the use of SCCs, GCCs, and cross-sector coordinating councils to create an integrated national framework for critical infrastructure protection and resilience across sectors.
- The networked approach to information sharing that provides for multidirectional exchanges of actionable intelligence, alerts, warnings, and other information between and among the various National Plan partners.

National Infrastructure Simulation and Analysis Center (NISAC)

The NISAC conducts modeling, simulation, and analysis of the nation's critical infrastructure, to include infrastructure risk, vulnerability, interdependencies, and event consequences. The Center's multidisciplinary expertise covers the full spectrum of the 16 critical infrastructure sectors while focusing on the challenges posed by interdependencies and the consequences of disruption. NISAC researchers and analysts conduct extensive modeling, simulation, and analysis to support risk mitigation and policy planning. They also provide real-time assistance to DHS decision-makers during response to such incidents as hurricanes, flooding, wildfires, and manmade events.

National Response Framework (NRF)

A guide to how the nation responds to all types of disasters and emergencies, the NRF is built on scalable, flexible, and adaptable concepts identified in the NIMS to align key roles and responsibilities across the nation. The framework describes specific authorities and best practices for managing incidents that range from the serious, but purely local, to large-scale terrorist attacks or catastrophic natural disasters. The NRF also describes the principles, roles, responsibilities, and coordinating structures for delivering the core capabilities required to respond to an incident, and further describes how response efforts integrate with those of the other mission areas defined in Presidential Policy Directive (PPD-8), National Preparedness.

National Risk Management Center (NRMC)

As CISA’s center for collaborative risk management, the NRMC works closely with the critical infrastructure community to identify and analyze the most significant risks to our Nation, and strategically manage resiliency and security efforts to “Secure Tomorrow.” Guiding the NRMC’s risk management efforts are the National Critical Functions (NCF)—the functions of government and the private sector that are so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety. Through collaborative efforts with the private sector, government agencies, and other key stakeholders, the NRMC uses a dynamic, cross-sector risk management process to identify, analyze, prioritize, and manage the most significant risks—cyber and physical—to those functions.

Presidential Policy Directive (PPD) 8

PPD-8: National Preparedness was released in March 2011 with the goal of strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation. PPD-8 defines five preparedness mission areas—Prevention, Protection, Mitigation, Response, and Recovery—and mandates the development of a series of policy and planning documents to explain and guide the Nation’s approach for ensuring and enhancing national preparedness.

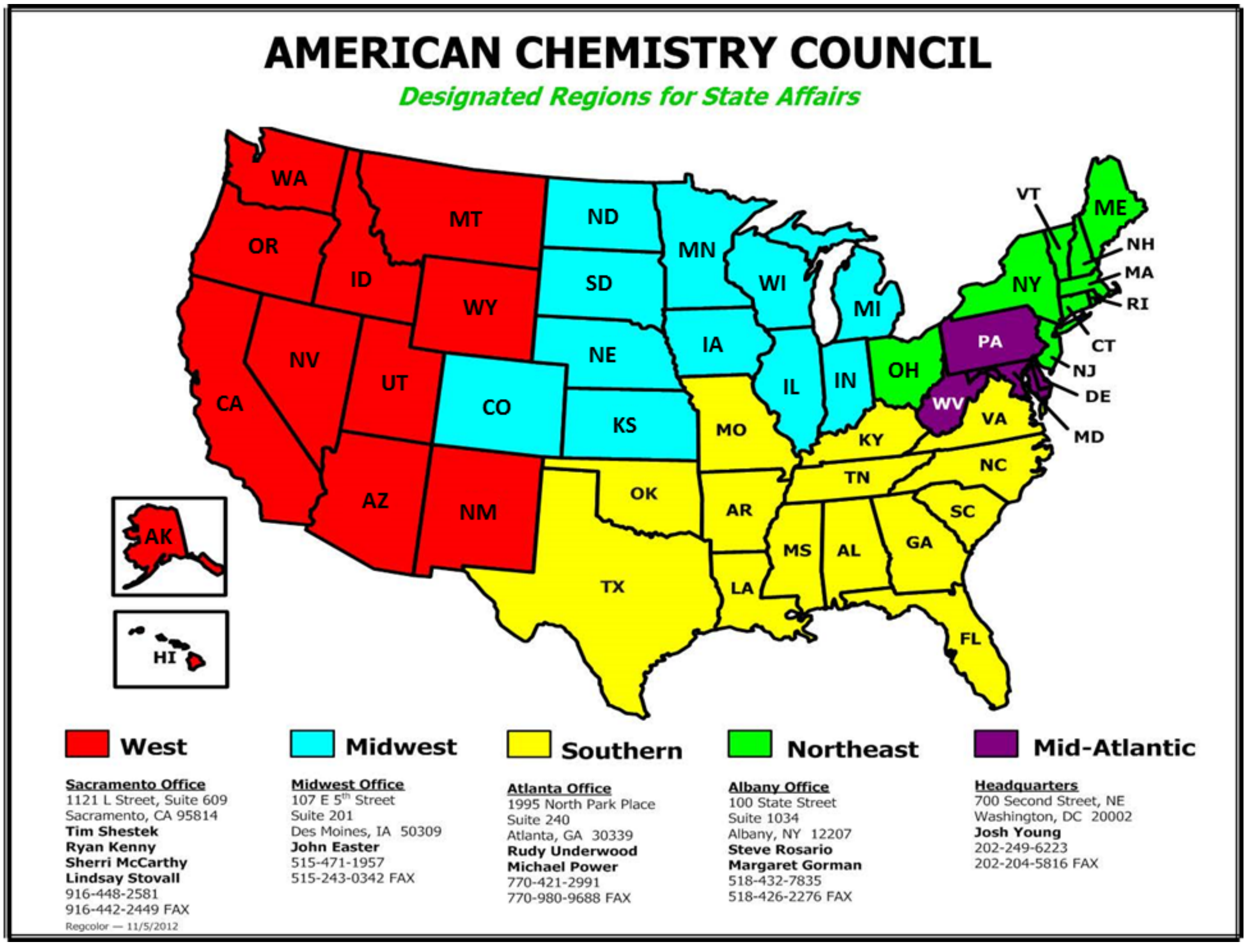
Sector Risk Management Agency

Recognizing that each critical infrastructure sector possesses its own unique characteristics, operating models, and risk landscapes, Presidential Policy Directive (PPD) 21 designates federal government SRMAs for each of the 16 critical infrastructure sectors. The SRMAs are responsible for working to implement the sector partnership model and risk management framework; develop protective programs, resiliency strategies, and related requirements; and provide sector-level protection guidance in line with the overarching guidance established by DHS pursuant to PPD-21. The Secretary of Homeland Security has delegated the SRMA responsibilities for the Chemical Sector to CISA. The Stakeholder Engagement Division (SED) within CISA , fulfills responsibility to implement voluntary chemical programs and the National Plan partnership model with the Chemical Sector.

APPENDIX K: AUTHORITIES

- *Defense Production Act, Public Law 115-232, 115th Congress,* August, 2018*.* https://www.fema.gov/sites/default/files/2020-03/Defense_Production_Act_2018.pdf (accessed March 2022).
- *Homeland Security Act of 2002, Public Law 107-296, 107th Congress,* November 25, 2002*.* https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf (accessed March 2022).
- *National Defense Authorization Act, H.R.4350 — 117th Congress,* October 18, 2021*.* https://www.congress.gov/bill/117th-congress/house-bill/4350/text (accessed March 2022).
- *Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), Public Law 93-288,* May 1, 2021*.* https://www.fema.gov/disaster/stafford-act (accessed March 2022).
- The White House, *Homeland Security Presidential Directive 5, Management of Domestic Incidents*, Washington, D.C. February 28, 2003. https://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf (accessed March 2022).
- The White House, *Presidential Policy Directive 8, National Preparedness*, Washington, D.C. March 30, 2011. https://www.dhs.gov/presidential-policy-directive-8-national-preparedness (accessed March 2022).
- The White House, *Presidential Policy Directive 21, Critical Infrastructure Security and Resilience*, Washington, D.C. February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed March 2022).
- U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *National Cyber Incident Response Plan*, Washington, D.C. December 2016. https://www.cisa.gov/uscert/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pd (accessed March 2022).
- U.S. Department of Homeland Security, Federal Emergency Management Agency, *National Disaster Recovery Framework (Second Edition)*, Washington, D.C. June 2016. https://www.fema.gov/sites/default/files/2020-06/national_disaster_recovery_framework_2nd.pdf (accessed March 2022).
- U.S. Department of Homeland Security, Federal Emergency Management Agency, *National Response Framework (Fourth Edition)*, Washington, D.C. October 2019. https://www.fema.gov/sites/default/files/2020-04/NRF_FINALApproved_2011028.pdf (accessed March 2022).

APPENDIX L: DESIGNATED REGIONS FOR STATE AFFAIRS



AMERICAN CHEMISTRY COUNCIL

Designated Regions for State Affairs

🟥 **West**

Sacramento Office
1121 L Street, Suite 609
Sacramento, CA 95814
Tim Shestek
Ryan Kenny
Sherri McCarthy
Lindsay Stovall
916-448-2581
916-442-2449 FAX
Regcolor — 11/5/2012

🟦 **Midwest**

Midwest Office
107 E 5th Street
Suite 201
Des Moines, IA 50309
John Easter
515-471-1957
515-243-0342 FAX

🟨 **Southern**

Atlanta Office
1995 North Park Place
Suite 240
Atlanta, GA 30339
Rudy Underwood
Michael Power
770-421-2991
770-980-9688 FAX

🟩 **Northeast**

Albany Office
100 State Street
Suite 1034
Albany, NY 12207
Steve Rosario
Margaret Gorman
518-432-7835
518-426-2276 FAX

🟪 **Mid-Atlantic**

Headquarters
700 Second Street, NE
Washington, DC 20002
Josh Young
202-249-6223
202-204-5816 FAX

Page intentionally blank

E-mail questions regarding this SOP or questions about the Chemical Sector to ChemicalSector@cisa.dhs.gov.