



CISA
CYBER+INFRASTRUCTURE



Chemical Sector-Specific Agency Incident Management and Coordination Playbook

AUGUST 2019

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

CHEMICAL SECTOR SNAPSHOT

IMPACTS

<p>96% of goods manufactured in the U.S. in 2013 depended on products supplied by the Chemical Sector</p>	<p>866 million tons of chemical products were shipped in 2013</p>	<p>25% of 2013 U.S. GDP was supported by the Chemical Sector</p>	<p>12% of 2013 U.S. Exports were supported by the Chemical Sector</p>
--	--	---	--

REGULATION

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

OWNERS AND OPERATORS

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

FUNCTIONAL AREAS

<p>Manufacturing Plants</p>  <p>Convert raw materials into intermediate and end products</p>	<p>Transport Systems</p>  <p>Transport chemicals to/from manufacturing plants, warehouses, and end users</p>
<p>Warehousing/Storage</p>  <p>Provide downsized repackaging and storage</p>	<p>End Users</p>  <p>Typically consume the chemical purchased</p>

CHEMICAL SEGMENTS

 <p>Basic</p> <p>E.g., Sodium chloride, ethanol, & sulfuric acid</p>	 <p>Specialty</p> <p>E.g., Adhesives, sealants, flavors and fragrances, food additives, & explosives</p>	 <p>Pharmaceutical</p> <p>E.g., Medicines, biological products, diagnostic substances, & vitamins</p>	 <p>Consumer</p> <p>E.g., Soaps, detergents, bleaches, toothpaste, cosmetics, perfume, & paints</p>	 <p>Agricultural</p> <p>E.g., Fertilizers, pesticides, fungicides, insecticides, & herbicides</p>
--	--	---	--	---

CRITICAL SECTOR INTERDEPENDENCIES

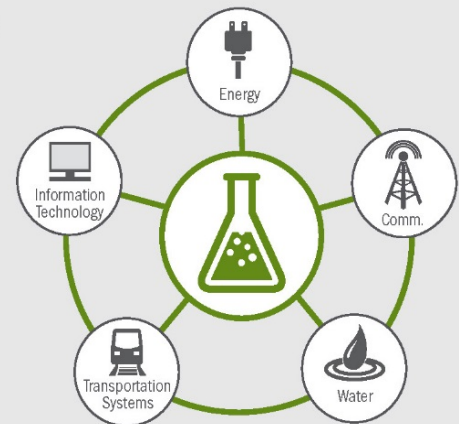
Water—Wastewater treatment and water purification processes rely on chemicals to make water safe, while chemical manufacturing requires large amounts of process and cooling water.

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.



Sector-Specific Incident Management Activation, Communication, and Engagement

Incident Management Roles

- ❑ The Cybersecurity and Infrastructure Security Agency (CISA) receives information about an actual or emerging incident that could affect one of the critical infrastructure sectors for which CISA serves as the sector-specific agency (SSA).
- ❑ CISA aggregates incident information and engages with the appropriate sector partners to validate preliminary assumptions and initial assessments.
- ❑ CISA determines the potential level of impacts based on the Incident Severity Schema for physical and cyber incidents (see below).
- ❑ CISA determines the appropriate sector-related actions and level of effort:
 - ❑ Maintain situational awareness and coordinate with sector partners through the established collaboration structures
 - ❑ Share information with sector stakeholders according to established protocols and information-sharing mechanisms
 - ❑ Conduct stakeholder engagements
 - ❑ Manage requests for information to and from sector stakeholders
 - ❑ Manage requests for assistance from sector stakeholders
 - ❑ Support U.S. Department of Homeland Security (DHS) and interagency reporting requirements

Incident Severity Schema

Physical or Cyber Incident Severity	Incident Severity Schema Description
Level 5 – <i>Emergency</i> (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 – <i>Severe</i> (Red)	Likely to result in a significant impact to critical infrastructure across multiple sectors/regions for a sustained period
Level 3 – <i>High</i> (Orange)	May have an impact on critical infrastructure function/operability across sectors/regions for a sustained period
Level 2 – <i>Medium</i> (Yellow)	May have an impact on critical infrastructure function/operability across sectors/regions for a sustained period
Level 2 – <i>Medium</i> (Green)	Unlikely to have an impact on critical infrastructure function/operability for a sustained period
Level 0 – <i>Baseline</i> (White)	Unsubstantiated or inconsequential event involving infrastructure assets

Contents

Introduction	1
Incident Management Activation	5
Inform	5
Validate.....	5
Activate	6
Incident Management and Coordination Practices.....	9
Preparedness	9
Response.....	10
Recovery	14
Appendix A. Incident Management Phases and Incident Severity Schema	16
Appendix B. SSA Coordination Across CISA Elements.....	18
Appendix C. Homeland Security Information Network – Critical Infrastructure	21
Appendix D. Information Security	22
Appendix E. Chemical Sector Partnership Council Member Organizations.....	23
Appendix F. Incident Teleconferences.....	24
Appendix G. Requests for Information and Requests for Assistance	26
Appendix H. Regulatory Waivers	27
Appendix I. National-Level Reporting	30
Appendix J. Authorities	32

Introduction

As the sector-specific agency (SSA) for the Chemical Sector, the Cybersecurity and Infrastructure Security Agency (CISA) is responsible for coordinating incident notification and sharing information among federal departments and agencies; state, local, tribal and territorial (SLTT) entities; and private-sector partners. CISA uses established systems and communication mechanisms to ensure the right information is available to decision-makers at the right time—before, during, and after incidents affecting the critical infrastructure sectors.

This document provides administrative and operational practices, easy-to-access tools and resources, and at-hand references to assist CISA—as the SSA for this critical infrastructure sector—in preparing for, responding to, and recovering from an all-hazards incident or event affecting the sector.

Chemical Sector-specific incident management and coordination activities may involve the direct participation of multiple elements across CISA, depending on the type of incident, its severity, and the need for a coordinated federal response. These elements typically include:

- **SSA Leadership:** CISA principal with the authority to direct resources in support of the SSA function.
- **SSA Management Team:** Organizational element within CISA that supports sector-specific strategic planning and coordination activities, manages national-level sector partnership structures and collaboration mechanisms, and provides the staffing function at the headquarters level in steady state as well as during incidents.
- **Regional Offices:** Operational elements of CISA at the regional level that provide targeted programs and services to owners and operators and coordinate regional information sharing.
- **CISA Integrated Operations Coordination Center (CIOCC):** Organization within CISA that serves as the primary information-sharing hub for incidents affecting critical infrastructure.
- **National Risk Management Center (NRMC):** Organization within CISA that serves as the lead for planning, analysis, and collaboration activities related to the most significant risks affecting critical infrastructure and critical functions.

Figure 1 depicts the coordination pathways between these elements. CISA leadership—as part of the SSA leadership role—oversees all incident management activities and may direct execution of sector-specific incident management and coordination activities by the CIOCC, regional offices, or SSA management team. The CIOCC combines communications, cyber, and physical infrastructure protection and resilience expertise, synchronized under a single operating concept. The CIOCC coordinates asset response during significant incidents and is the focal point for sharing information among federal and non-federal entities.

The NRMC identifies the infrastructure in the affected area that, if disrupted, could lead to national-level consequences. The NRMC also provides analytic products on direct incident impacts and cascading impacts, as well as tailored analysis requested by CISA leadership and other incident responders. For additional



Figure 1. Internal Coordination Mechanisms for Sector-Specific Incident Management

information on determining the need for a coordinated federal response and coordination across CISA elements, see Appendices A and B.

For all-hazards incidents, CISA—as the SSA for this critical infrastructure sector—is responsible for maintaining situational awareness, assessing and analyzing critical infrastructure data related to the sector, collaborating and coordinating with sector partners, sharing pertinent information with sector stakeholders, and responding to requests for information (RFIs) and requests for assistance (RFAs), as appropriate. The SSA roles and responsibilities executed by CISA during an incident (as depicted in Figure 2) include:

- **Information Sharing:** Collecting, synthesizing, prioritizing, and disseminating event-related information at the national, regional, and local levels; facilitating access to federally produced pre- and post-event impact analyses and modeling products; and managing and sharing information on the Homeland Security Information Network – Critical Infrastructure (HSIN-CI). For information on HSIN-CI and the use of information designations, see Appendices C and D.
- **Partnership Coordination and Collaboration:** Coordinating incident situational awareness between CISA and the organizations that comprise the corresponding partnership councils: the Government Coordinating Council (GCC) and Sector Coordinating Council (SCC). For a list of partnership council member organizations, see Appendix E.
- **Stakeholder Engagement:** Conducting outreach engagements with sector stakeholders at the national, regional, and local levels to collect or provide incident information and response options for consideration. Outreach engagements may be conducted under a variety of formats, including email, teleconference, video teleconference, or in-person meetings. For additional information on the use of calls and briefings, see Appendix F.
- **Requests for Information/Assistance:** Supporting and facilitating the submittal, processing, and tracking of RFIs and RFAs from sector stakeholders (at the national, regional, and local levels) to the CIOCC. For additional information on processing requests, including those related to regulatory waivers, see Appendices G and H.
- **Internal Reporting and Interagency Coordination:** Reporting incident status, critical infrastructure impacts, response activities, and federal resource commitments to the DHS, as well as coordinating with other federal partners as required. For additional information on national-level reporting, see Appendix I.

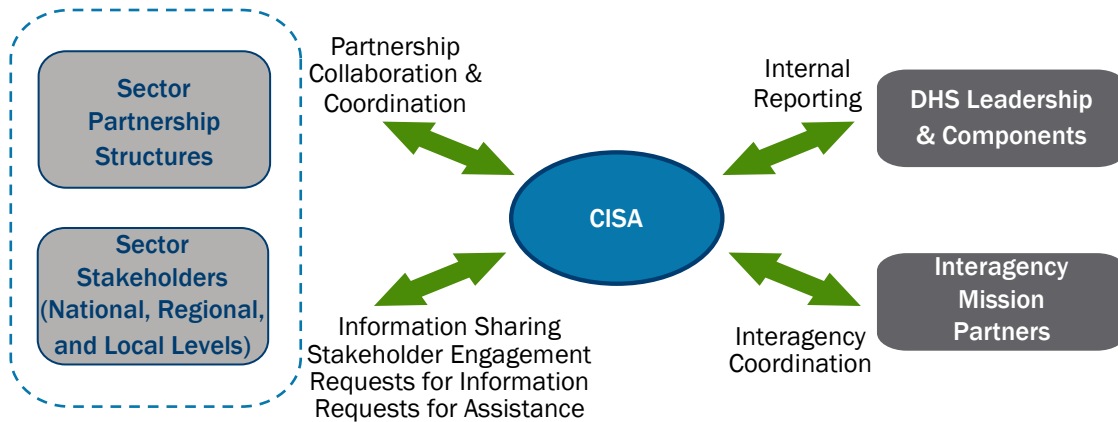


Figure 2. SSA Roles and Responsibilities for Sector-Specific Incident Management and Coordination

About the Incident Management and Coordination Playbook

The *Chemical Sector-Specific Agency Incident Management and Coordination Playbook* (playbook) provides administrative and operational practices, easy-to-access tools and resources, and at-hand references to assist CISA—as the SSA for this critical infrastructure sector—in preparing for, responding to, and recovering from an all-hazards incident or event affecting the sector. These practices, resources, and references are based on current DHS policy and guidance.

The playbook applies to both advance-notice and no-notice physical or cyber events that trigger a coordinated response between the Federal Government and its sector partners. The intended audience for the playbook includes those organizations within CISA with roles and responsibilities in support of the SSA function. Though these organizations may be assigned other incident response duties as CISA elements, the playbook pertains only to the roles and responsibilities in support of the SSA function.

The playbook is organized into five major sections, described below. It may be read in its entirety, or sections of the playbook can be removed for use for a specific incident, relating to the responsibilities assigned to specific elements within CISA:

- **Incident Management Activation and Communication:** Highlights the major steps of activation for an incident or event. This section includes established criteria for decision-making about responses to an incident, contact information necessary to support the incident, and a sector snapshot.
- **Introduction:** Highlights the overarching responsibilities of the SSA for all-hazards incident management and coordination.
- **Activation:** Describes the process by which the SSA activates its incident management and coordination protocols.
- **Incident Management and Coordination Practices:** Lists the administrative and operational practices of the SSA to support three stages of incident management: preparedness, response, and recovery.
- **Appendices:** Provide readily accessible reference material to carry out incident management and coordination practices, including incident severity determination, coordination across DHS components, incident teleconferences, HSIN-CI, RFIs and RFAs, information security, national-level reporting, regulatory relief, and statutory authorities.

The practices described in the playbook utilize the unified risk-based approach and partnership model framework for steady-state protection detailed in the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013). The contents of the playbook reflect lessons learned gathered over years of experience with joint exercise activities and real-world emergencies that required a coordinated public-private sector response. Although it is designed to provide as much specific guidance as possible, this playbook is also intended to be dynamic, flexible, and tailored in its application to accommodate the unique aspects of an event scenario. The playbook is also designed to adhere to the unique authorities, capabilities, and decision-making processes of the various partner organizations that must work together to effect a well-coordinated response.

Terms and Definitions

For purposes of the playbook, an incident or event is an occurrence—natural or man-made—that:

- Represents a significant change from normal, steady-state conditions of a critical infrastructure facility or system, or
- May require a response to protect life or property and minimize potential adverse consequences, or
- May require protective measures to mitigate vulnerabilities to the critical infrastructure facility or system that may be threatened by the incident.

All-hazards incidents may be natural or man-made, can be localized or widespread, may affect physical or cyber infrastructure, and have a variety of primary and secondary consequences. All-hazards incidents can be characterized as either advance-notice or no-notice. A no-notice incident occurs unexpectedly or with minimal warning. Some examples of no-notice incidents include earthquakes, tsunamis, blackouts, and terrorist attacks. It is also possible that incidents with typically predictable patterns can become no-notice incidents when their behavior differs from what is expected. The specific nature of the event will determine the appropriate course of action taken by either the SSA, as outlined in this playbook, or other responsible parties. A list of events is included in Table 1.

Acknowledgements, Distribution, and Maintenance

The development of the *Chemical Sector-Specific Agency Incident Management and Coordination Playbook* was led by the SSA management team, in consultation with the GCC and SCC. The playbook was developed pursuant to the sector partnership framework described in the [NIPP 2013](#) and is designed to implement the concept of operations described in the [Critical Infrastructure and Key Resources Support Annex to the National Response Framework](#) (NRF) and the [National Cyber Incident Response Plan](#) (NCIRP).

Sector partners and related personnel should use appropriate measures to ensure the proper use and maintenance of this information. The playbook will be reviewed at least every other year and tested as appropriate (e.g., at a national-level exercise or other large-scale exercise) to remain current and compliant with policy and general practice changes. The SSA management team will review any proposed changes or revisions to the playbook and approve or reject them. Extensive revisions to the National Planning Frameworks, the NIPP 2013, the NCIRP, the National Incident Management System (NIMS), Federal Interagency Operational Plans, or other national-level guidance on cyber and physical incident management—as well as significant revisions to CISA’s organizational or operational structure—may require changes to key elements of the playbook.

Table 1. Sample Event Types and Potential Scenarios

Slow-Onset Events
<ul style="list-style-type: none"> • Climatological Events (extreme temperatures, drought, wildfires) • Hydrological Events (floods) • Meteorological Events (tropical cyclones, severe winter storms) • Pandemics (global disease outbreaks) • Space Weather Events (geomagnetic storms) • Scheduled Disruptions (shutdowns for maintenance, upgrade, or rehabilitation)
No-Notice Events
<ul style="list-style-type: none"> • Criminal Incidents and Terrorist Attacks (vandalism, theft, property damage, active shooter incidents, kinetic attacks) • Cyber Incidents (denial-of-service attacks, zero-day exploits, malware, phishing) • Geophysical Events (earthquakes, tsunamis, volcanic eruptions) • Hydrological Events (flash floods) • Technological and Industrial Accidents (structural failures, industrial fires, hazardous substance releases, chemical spills) • Meteorological Events (severe convective storms) • Unscheduled Disruptions (equipment malfunction, long-term power outages)

Incident Management Activation

Before, during, and after an incident, the need for assistance or information can originate from many different entities from the local level to the federal level. The incident information may follow a number of paths through the distributed network of stakeholders and interagency partners before reaching CISA. CISA must then validate that information, potentially combining it with other sources for further analysis. The origin and the evaluation of incident information may differ slightly for physical versus cyber incidents. For either type of incident, CISA leadership will direct the appropriate level of effort to support the sector directly or through the coordinated federal response. Figure 3 below summarizes these steps, from discovering a threat or incident to activating a sector-specific response.



Figure 3. Process of activation in all-hazards response

Inform

Critical infrastructure sectors generally comprise a broad range of entities that take advantage of multiple communication channels that facilitate information sharing when an actual or potential incident occurs. For example, a sector stakeholder may request information or assistance through the CIOCC or the regional offices, while sector partners actively engaged in the sector partnership council structure may directly engage the SSA management team. At the same time, these organizational elements may share with sector stakeholders threat information received through the DHS Office of Intelligence and Analysis or analytical products developed by the NRMCC, as appropriate.

Incident-related requests for information and assistance may flow from a regional or headquarters nexus, with differences in whether sector entities are directly or indirectly affected. For example, for a specific sector entity directly affected by a physical incident, information sharing and assistance would likely be directed out of the appropriate regional office and would also flow to other critical infrastructure entities indirectly affected because of their proximity to the incident. In the case of an entity affected by a cyber incident, assistance would flow from the CIOCC, and the SSA management team would coordinate at the headquarters level to share information with other stakeholders, as appropriate.

Validate

CISA evaluates the situation and confirms the need to respond by leveraging many sources for information and analysis. Specific discussions with key sector partners may be conducted through the established sector partnership mechanisms. The CIOCC generates shared situational awareness across sectors for physical and cyber incidents and may supplement the initial incident information with additional information and analysis provided by stakeholders. The CIOCC collaborates with federal departments and agencies (including the SSAs), SLTT entities, and sector partners to compile actionable information and evaluate the severity of incidents.

For physical and cyber incidents, the CIOCC will assess the severity level according to its Incident Severity Schema. This schema describes the likelihood of significant impact on critical infrastructure operations with levels that range from Level 0: Baseline to Level 5: Emergency. Appendix A provides more detail on the Severity Schema.

Activate

CISA employs three incident management phases—Guarded, Concern, and Urgent—to effect efficient use of available resources. Each successive phase corresponds to increasing significance and complexity of the anticipated level of effort. However, progression through the phases is not linear, and senior leadership may set or change phases to match the requirements for responding to a given incident as it evolves. Incidents fall into one of two categories:

- **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. Slow-onset or advance-notice events may suddenly change from Guarded or Concern to the Urgent incident management phase.
- **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

Ultimately, CISA leadership considers the severity level established by the CIOCC, as well as incident information and assessments from headquarters and the regional office(s), when determining the appropriate level of coordination with the sector. These factors also inform CISA support to any coordinated federal response. The phase determination activates the various mechanisms outlined in this playbook and other standard operating procedures (SOPs).

As the SSA, 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 Incident Severity Schema).

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, the CIOCC maintains its 24–7 watch operations and shares information with the SSA management team and the regional offices through established protocols. Both physical and cyber incident information pertinent to the sector flow through the CIOCC. Physical and cyber incident information pass through respective components of the CIOCC. RFIs and RFAs for incidents are routed and managed through the CIOCC and may relate to various topics, including those listed in Table 3 to the right. For more information on RFIs and RFAs, see Appendix G.

For significant incidents that require a coordinated federal response, the CIOCC acts as the central coordinating entity providing situational awareness and integrated actionable information for incidents affecting critical infrastructure. The CIOCC collects information from and shares information with the SSA management team and the regional offices, which serve as conduits of information between the CIOCC and sector stakeholders. The SSA management team and the regional offices use their established information-sharing mechanisms to coordinate with sector stakeholders. The CIOCC may host subject matter experts (SMEs) from the SSA management team as part of their day-to-day operations, as appropriate.

The CIOCC 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
<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • 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. SSA Activation

Activation Step	Activities
Inform	Affected entities may submit incident information through the SSA management team, through a regional office, or directly to the CIOCC. Affected entities are encouraged to contact the CIOCC directly for asset response.
Validate	The CIOCC assesses the severity of the incident against established criteria, assessing both physical and cyber impacts, and informs CISA leadership.
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.

Figure 4, below, provides an example email message from the CIOCC, sending notification of the change in CISA’s operational posture to Phase 1: Guarded for a specific incident.

From: CIOCC
 Subject: (FOUO) CISA Phase 1 GUARDED Warning Order – [Topic/Incident Name]
 FOR OFFICIAL USE ONLY
 The Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), will elevate its operational posture and transition to Phase 1 GUARDED, effective immediately, in response to [Topic/Incident Description].
 An activation of the CISA Crisis Action Team is not ordered at this time.
 This order will remain in effect until modified or terminated.
 If you have any questions or concerns about this matter, contact the CIOCC at 202-282-9201 or ciocc@cisa.dhs.gov.
 V/r,
 CIOCC Watch Operations
 Department of Homeland Security
 202-282-9201
 Email: ciocc@cisa.dhs.gov
 FOR OFFICIAL USE ONLY

Figure 4. Example CIOCC Notification Email

Incident Management and Coordination Practices

To effectively support incident management and coordination, the SSA management team conducts 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

In advance of an incident, the SSA management team undertakes a variety of administrative and operational activities, including updating contact information, reading and monitoring key resources and information, and integrating continual process improvement into preparation plans and activities. This section illustrates the administrative and operational practices undertaken in the preparedness stage to support timely and effective response during an event.

Administrative

- Review pre-season/pre-cycle impacts analysis and modeling provided by the NRMCM and other federal agencies, when available.
- Update the GCC, SCC, and other agency contact lists.
- Identify changes to relevant statutory and regulatory programs, potential capabilities, and limiting factors pertaining to response and recovery support for infrastructure systems.
- Establish awareness of industry emergency shut-down processes and related needs.
- Review relevant changes to CISA (or other federal, state, or local department/agency) policies, plans, and procedures with a potential impact on sector information-sharing and incident-response capabilities/activities.
- Transition from preparation to event response upon notification that an event is nearing the impact stage (e.g., hurricane landfall).

Operational

Information Sharing

- Share available NRMCM and other federal agency pre-season/pre-cycle impacts analysis and modeling with sector partners via established information-sharing mechanisms (e.g., HSIN-CI).
- Create a HSIN Connect situation room, if applicable, and configure the various share pods (e.g., notes, chat, share, attendee list, web links, and file share).

Partnership Coordination and Collaboration

- Collaborate with regional office(s) and sector partners to identify critical facilities, assets, functions, and interdependencies to reduce risk pre- and post-event.

Stakeholder Engagement

- Schedule pre-incident sector-specific teleconference calls (unclassified and classified, as needed or requested, and conducted at appropriate intervals for the event) with sector partners at the national level (e.g., the GCC, SCC, information-sharing and analysis centers [ISACs], and all sector stakeholders) and regional office(s). For additional information, see Appendix F.
- Leverage pre-existing meetings, teleconferences, or webinars scheduled with sector stakeholders to schedule engagements for the specific event or incident.

Requests for Information

- Respond to RFIs to support sector-related preparedness activities. RFIs may include hazard/infrastructure analysis and modeling, existing risk assessments, or sector status reports for situational awareness. For additional information, see Appendix G.

Response

The SSA management team's administrative and operational responsibilities in response to an all-hazards event include reviewing, monitoring, and contributing to analysis of the event, as well as communication with industry and government partners. All-hazards events fall into one of two categories: slow-onset or advance-notice events, which can be forecasted more than 72 hours prior to impact, and no-notice events, which occur with little to no warning, thus limiting the opportunity to prepare. While CISA may assign any phase to an event as necessary, the operational phases are not linear. Changes in operational phase may occur in response to incident and information requirements. The response to no-notice events may initiate at Phase 2: Concern or Phase 3: Urgent.

Slow-Onset or Advance-Notice Events

CISA will activate Phase 1 (Guarded) when the weather forecast or another information source identifies an intense or rapidly strengthening low-pressure storm system (i.e., a tropical storm/hurricane watch or warning or a severe winter storm). Phase 1 also applies in the early stages of other advance-notice events with the potential to require a coordinated public-private response (see Table 1 in the Introduction for a list of possible events). Phase 2 will follow as the likely event nears. For these types of all-hazards events, the SSA management team will engage in the following administrative and operational practices.

Administrative

- Review analytical and modeling products developed by the NRMC and other federal agencies, when available.
- Update sector council (e.g., GCC, SCC) and other agency contact lists.
- Notify sector council members of any cross-sector teleconference calls scheduled for the event.
- Remind sector council members to update HSIN access information, including user name and password information.
- Transition from preparation to event response upon notification that an event is nearing the impact stage (e.g., hurricane landfall).
- Adhere to appropriate and required mechanisms for safeguarding sensitive and classified information. For additional information, see Appendix D.

Operational

Phase 1: Guarded (72–96 hours prior to event impact)

Information Sharing

- Identify and share with sector stakeholders the defined severity of the incident (e.g., emergency, severe, high, medium, or low). For additional information, see Appendix A.
- Share incident-related information and available products with sector stakeholders via email, HSIN-CI, and/or ISAC(s), as appropriate.
- Communicate with sector stakeholders regarding incident-related postings on HSIN-CI to ensure awareness of updated information.
- Share information received from sector partners at the national level with the CIOCC and regional office(s), as appropriate.
- Maintain the HSIN Connect situation room (if created).

Partnership Coordination and Collaboration

- Support NRMCC development of an infrastructure of concern (IOC) list to identify significant critical infrastructure that could be affected by the incident. Collaborate with regional office(s) to obtain input.
- Collaborate with regional office(s) and sector partners to identify potential critical infrastructure impacts, interdependencies, cascading effects, and redundancies relevant to the incident.
- Collaborate with regional office(s) to share incident information with Federal Emergency Management Agency (FEMA) offices (local, regional, headquarters), as appropriate.
- Request information from sector partners regarding sector impacts and corresponding prevention, protection, mitigation, response, and recovery actions they are taking. For additional information, see Appendices F and G.
- Engage cross-sector councils to identify any other sectors that may be affected by the event; engage SMEs in other sectors, as appropriate, to obtain critical information to contribute to intra-sector and cross-sector analyses.

Stakeholder Engagement

- Schedule pre-incident sector-specific teleconference calls (unclassified and classified, as needed or requested, and conducted at appropriate intervals for the event) with sector partners at the national level (e.g., the GCC, SCC, ISAC(s), and all sector stakeholders) and regional office(s). For additional information, see Appendix F.

Requests for Information

- Respond to RFIs and RFAs for Phase 1 response, which may include:
 - RFI: Hazard/infrastructure analysis and modeling, existing risk assessments, or sector situational awareness
 - RFA: Site security or pre-positioning of response and recovery resources
- Coordinate with CIOCC for processing of RFIs and RFAs directed to the SSA management team. For additional information, see Appendix G.

Internal Reporting and Interagency Coordination

- Support internal reporting processes established for the incident.
- Coordinate with interagency partners to ensure reporting consistency, as appropriate.

Operational

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

Information Sharing

- Identify and share with sector stakeholders the defined severity of the incident (e.g., significant, non-significant), noting any changes from Phase 1. For additional information, see Appendix A.
- Share incident-related information and available products with sector stakeholders via email, HSIN-CI, and/or ISAC(s), as appropriate.
- Continue to communicate with sector stakeholders regarding incident-related postings on HSIN-CI to ensure awareness of updated information.
- Share information received from sector partners at the national level with the CIOCC and regional office(s), as appropriate.
- Maintain the HSIN Connect situation room (if created).

Partnership Coordination and Collaboration

- Collaborate with NRMC and regional office(s) to modify or refine the IOC list, as appropriate, identifying any new information or changes from Phase 1.
- Continue to collaborate with regional office(s) and sector partners to identify potential critical infrastructure impacts, interdependencies, cascading effects, and redundancies relevant to the incident.
- Continue to collaborate with regional offices to share incident information with FEMA offices (local, regional, headquarters), as appropriate.
- Support regional office(s) in their efforts to engage with regional stakeholders in the potential impact area to identify potential impacts, concerns, and priorities.
- Request information from sector partners regarding sector impacts and corresponding prevention, protection, mitigation, response, and recovery actions they are taking. For additional information, see Appendices F and G.
- Continue to engage SMEs in other sectors that may be affected by the event, as appropriate, to obtain critical information to contribute to intra-sector and cross-sector analyses.

Stakeholder Engagement

- Schedule pre-incident sector-specific teleconference calls (unclassified and classified, as needed or requested, and conducted at appropriate intervals for the event) with sector partners at the national level (e.g., the GCC, SCC, ISAC(s), and all sector stakeholders) and regional office(s). For additional information, see Appendix F.

Requests for Information

- Respond to RFIs and RFAs for Phase 2 response, which may include:
 - RFI: Hazard/infrastructure analysis and modeling, existing risk assessments, or sector situational awareness
 - RFA: Site security or pre-positioning of response and recovery resources
- Coordinate with CIOCC for processing of RFIs and RFAs directed to the SSA management team. For additional information, see Appendix G.

Internal Reporting and Interagency Coordination

- Support internal reporting processes established for the incident.
- Coordinate with interagency partners to ensure reporting consistency, as appropriate.

Urgent/No-Notice Events

Urgent or no-notice events are sudden (little to no warning), which limits the ability to prepare in advance. These types of events can take the form of a natural disaster (e.g., tornado or earthquake), an industrial accident, or a man-made/intentional act of sabotage or terrorism resulting in a cyber incident and/or infrastructure failure. Response to a no-notice event at the federal level will be incident-specific. Once notified by the CIOCC that the emergency response for the event is at the national level, the SSA management team notifies GCC and SCC leadership of the need to implement various processes and mechanisms outlined in this playbook and other SOPs. For no-notice events, the SSA management team will engage in the following operational activities.

Operational

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

Information Sharing

- Identify and share with sector stakeholders the defined severity of the incident (e.g., emergency, severe, high, medium, or low), noting any changes. For additional information, see Appendix A.
- Share incident-related information and available products with sector stakeholders via email, HSIN-CI, and/or ISAC(s), as appropriate.
- Communicate with sector stakeholders regarding incident-related postings on HSIN-CI to ensure awareness of updated information.
- Share information received from sector partners at the national level with the CIOCC and regional office(s), as appropriate.
- Maintain the HSIN Connect situation room, (if created).

Partnership Coordination and Collaboration

- Collaborate with NRMC and regional office(s) to modify or refine the IOC list, as appropriate, identifying any new information or changes from Phase 2.
- Collaborate with regional office(s) and sector partners to identify potential critical infrastructure impacts, interdependencies, cascading effects, and redundancies relevant to the incident.
- Collaborate with regional offices to share incident information with FEMA offices (local, regional, headquarters), as appropriate.
- Support regional office(s) in their efforts to engage with regional stakeholders in the potential impact area to identify potential impacts, concerns, and priorities.
- Request information from sector partners regarding sector impacts, any associated responses, and recovery actions they are taking. For additional information, see Appendices F and G.
- Engage SMEs in other sectors that may be affected by the event, as appropriate, to obtain critical information to contribute to intra-sector and cross-sector analyses.
- Coordinate with regional office(s) and sector partners at the national level, and determine the status of any mandatory evacuations and establishment of evacuation routes, as appropriate.

Stakeholder Engagement

- Schedule sector-specific teleconference calls (unclassified and classified, as needed or requested, and conducted at appropriate intervals for the event) with sector partners at the national level (e.g., GCC, SCC, ISAC(s), and all sector stakeholders) and regional office(s). For additional information, see Appendix F.

Requests for Information

- Respond to RFIs and RFAs for Phase 3 response, which may include:
 - RFI: Hazard/infrastructure analysis and modeling, real-time risk or impact assessments, or sector situational awareness
 - RFA: Site security, impact area access, fuel coordination, positioning of response and recovery resources, or accommodations for crews needed to perform critical repair/restoration of service work
- Coordinate with the CIOCC for processing of RFIs and RFAs directed to the SSA management team. For additional information, see Appendix G.

Internal Reporting and Interagency Coordination

- In the case of a cyber incident defined as significant, support CISA/ISD leadership participation in the Cyber Unified Coordination Group (UCG), as appropriate.
- Support internal reporting processes established for the incident. If applicable, provide information on event impacts on the sector to the CIOCC for national-level reporting (NLR). For additional information on NLR, see Appendix I. Information types include:
 - 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
- Coordinate with interagency partners to ensure reporting consistency, as appropriate.

Recovery

During the recovery stage, the SSA management team monitors and ensures the flow of up-to-date information, facilitates communication flow between appropriate partners, and supports transition back to steady-state operations. 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. Depending on the event and the specific components of critical infrastructure, recovery and response may occur simultaneously. CISA leadership directs termination of recovery-focused collaboration and coordination activities as appropriate, based on mission assignments (e.g., ending CIOCC recovery activities for an incident); decision-making at this stage may involve consultation with sector council leadership. For recovery, the SSA management team will engage in the following administrative and operational activities.

Administrative

- Identify changes to relevant statutory and/or regulatory programs, potential capabilities, and/or limiting factors pertaining to recovery support for infrastructure systems.
- Transition from event response to recovery, as directed by CISA leadership in consultation with sector council leadership.
- Coordinate with regional office(s) and sector partners at the national level to gather lessons learned and recommendations of best practices to update this playbook, training, and other guidance.

Operational

Information Sharing

- Review available damage assessment and status reports to inform identification of infrastructure restoration priorities.
- Share incident-related information and available products with sector stakeholders via email, HSIN-CI, and/or ISAC(s), as appropriate.
- Maintain the HSIN Connect situation room (if created).

Partnership Coordination and Collaboration

- Provide sector-specific knowledge and expertise to regional office(s) and sector partners to support recovery activities including security needs, safe zones, escorts, reentry access, and other critical needs such as electricity, essentials, emergency housing, and communications.
- Collaborate with regional office(s) and sector partners to ensure that sector infrastructure is recovered in a timely and efficient manner to minimize the impact of service disruptions.

Stakeholder Engagement

- Schedule sector-specific teleconference calls (unclassified and classified, as needed or requested, and conducted at appropriate intervals for the event) with sector partners at the national level (e.g., the GCC, SCC, ISAC(s), and all sector stakeholders) and regional office(s). For additional information, see Appendix F.

Requests for Information

- Monitor the status of outstanding RFIs and RFAs, and provide updates to sector stakeholders, as appropriate. For additional information, see Appendix G.

Internal Reporting and Interagency Coordination

- Provide sector-specific knowledge and expertise to interagency partners to inform identification of infrastructure restoration priorities.
- Coordinate with interagency partners to ensure reporting consistency, as appropriate.

Appendix A. Incident Management Phases and Incident Severity Schema

The Cybersecurity and Infrastructure Security Agency (CISA) defines three incident management phases to outline the operational response and to maximize the efficient and effective use of available resources to support the agency's critical infrastructure partners.

The nature and severity of an incident, whether physical or cyber, helps determine the degree of coordinated federal response. A schema for describing incident severity establishes a common framework to evaluate and assess both physical and cyber incidents. The CISA Integrated Operations Coordination Center (CIOCC) uses its own Incident Severity Schema. All departments and agencies can employ the schema to ensure a common view of incident severity, the urgency required for responding, the seniority level necessary for coordinating response efforts, and the level of investment required for response efforts.

CISA Incident Management Phases

The incident management phases, listed below, are divided into categories of increasing significance, complexity, and level of anticipated effort.

- **Enhanced Awareness:** Assessment of information following notification of actual or potential incidents, events, and threats.
- **Phase 1 (Guarded):** Assessment and information sharing on:
 - Potential or actual incidents affecting critical infrastructure
 - Threats of national significance
 - Incidents of interest to CISA leadership
 - Incidents requiring coordination between two or more CISA divisions
 - Anticipation of a significant notice event
- **Phase 2 (Concern):** Assessment and information sharing on credible threats or large-scale incidents:
 - Affecting nationally significant critical infrastructure
 - In response to increased requirements for national-level reporting
- **Phase 3 (Urgent):** Assessment and information sharing on an incident so catastrophic that the Federal Government must assume the highest level of activity.

Although these phases align very closely with the operational phases used by the National Operations Center and the activation levels of the National Response Coordination Center, CISA assesses the impact of a potential or emerging incident or event independently and determines the appropriate incident management phase to maximize the efficient and effective use of available resources to support its critical infrastructure partners. A phase change ensures CISA is prepared to provide the appropriate level of support to the response by increasing the operational tempo (pace of operations) of the organization as a whole, establishing an operational rhythm for incident management personnel, and assigning/deploying personnel to incident management locations involved in response and recovery efforts (including field operating locations). Incidents determined as Phase 1 or higher require a coordinated federal response.

These incident management phases are not linear; phase changes occur in response to incidents and information requirements and may move forward or backward as a result of sudden and unpredictable developments. CISA may also skip phases in response to no-notice incidents during which the initial response occurs at Phase 2 (Concern) or Phase 3 (Urgent).

Incident Severity Schema

For response to incidents that affect critical infrastructure, including both cyber and physical incidents, the CIOCC Watch employs the Incident Severity Schema displayed in Table A1. The CIOCC Watch evaluates an incident and assigns a severity level, which informs CISA’s decisions about the level of response to an incident.

Table A1. CISA Incident Severity Schema

Physical or Cyber Incident Severity	Incident Severity Schema Description
Level 5 – <i>Emergency</i> (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 – <i>Severe</i> (Red)	Likely to result in a significant impact to critical infrastructure across multiple sectors/regions for a sustained period
Level 3 – <i>High</i> (Orange)	Likely to result in a demonstrable impact to critical infrastructure across sectors/regions for a sustained period
Level 2 – <i>Medium</i> (Yellow)	May impact critical infrastructure functioning across sectors/regions for a sustained period
Level 1 – <i>Low</i> (Green)	Unlikely to impact critical infrastructure function/operability for a sustained period
Level 0 – <i>Baseline</i> (White)	Unsubstantiated or inconsequential event involving infrastructure assets

The schema aligns with the National Cyber Incident Response Plan and Presidential Policy Directive 41 (PPD-41): *United States Cyber Incident Coordination* for response to cyber incidents. A cyber incident is an event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. A significant cyber incident is a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

Appendix B. SSA Coordination Across CISA Elements

Sector-specific agency (SSA) incident management and coordination practices can span multiple components across the Cybersecurity and Infrastructure Security Agency (CISA). The following is a summary of different CISA components and their general incident management and coordination roles as they pertain to the SSA function. Please refer to each component's incident management policy and guidance for additional information on the component's broader mission and responsibilities.

CISA Integrated Operations Coordination Center

The CISA Integrated Operations Coordination Center (CIOCC) provides situational awareness, facilitates information sharing, and coordinates unity of effort 24 hours a day, 7 days a week (24-7) to ensure the protection and resilience of the Nation's critical infrastructure. The CIOCC serves as the focal point for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect physical critical infrastructure.

CIOCC performs the following incident management and coordination responsibilities in support of CISA's role as the SSA for this critical infrastructure sector:

- Serving as the centralized mechanism for critical infrastructure situational awareness and information sharing, as well as the coordination of requests for information (RFIs) and requests for assistance (RFAs) through the CIOCC Watch and Warning, for regional offices and field personnel and critical infrastructure partners.
- Managing CISA's alert and warning system during emerging and actual incidents and events.
- Providing CISA-wide contingency and crisis action planning through the CIOCC Planning Branch.
- Managing the operational readiness and surge capability of the CISA-Crisis Action Team (CAT).
- Providing personnel, as required, to augment the CISA-CAT and provide support to other interagency functions.

SSA Management Team

The SSA management team coordinates activities among the government coordinating councils, sector coordinating councils, the other SSAs, critical infrastructure owners and operators, and other sector partners.

The incident management and coordination responsibilities performed by the SSA management team in support of CISA's role as the SSA for this critical infrastructure sector include:

- Leading sector-specific teleconference calls for incidents not associated with the surge of the CISA-CAT (more information on the calls can be found in the *Critical Infrastructure Stakeholder Teleconference Call Standard Operating Procedure*).
- Providing subject matter expertise on critical lifeline functions, critical infrastructure sectors, and cross-sector interdependencies.
- Facilitating coordination with sector stakeholders for other CISA elements.
- Monitoring incident activity to maintain situational awareness and posting incident-related documents on the Homeland Security Information Network – Critical Infrastructure (HSIN-CI).
- Providing recommended protective measures to sector stakeholders in the public and private sectors, to assist in reducing risk.

- Providing situational awareness and information to the CIOCC.
- Ensuring all applicable alerts and warnings issued by the CIOCC are shared through the established information-sharing and collaboration mechanisms.
- Creating a Situation Room in HSIN Connect, to serve as the sector-specific incident dashboard to support sector stakeholders and respond to industry requests for information.

Regional Offices

CISA established regional offices across the country to improve the delivery of the department's services to critical infrastructure owners and operators and state, local, tribal, and territorial (SLTT) partners and to enhance support to existing CISA field staff. The regional offices execute the following incident management and coordination responsibilities in support of CISA's role as the SSA for this critical infrastructure sector:

- Targeted delivery of services, especially in response to evolving threats and incidents
- Stronger coordination with local officials for exercises, training, and planning
- Deeper understanding of each region's risks, stakeholders, and requirements, allowing for customized advice and expertise on critical infrastructure security, resilience, and recovery
- Tailored outreach to and engagements with industries and sectors that are prevalent in a specific region
- Integrated physical and cyber threat mitigation
- Improved response time to stakeholder requests for information and services

Protective Security Advisors

As members of regional offices, protective security advisors (PSAs) are security subject matter experts who engage with SLTT government mission partners and members of the private-sector stakeholder community to protect the Nation's critical infrastructure. PSAs play an essential engagement and outreach role through their direct interactions with sector stakeholders affected by an incident. PSAs also serve as a link to DHS infrastructure protection resources; coordinate vulnerability assessments, training, and other DHS products and services; facilitate information sharing in steady state and incident response; and assist facility owners and operators with obtaining security clearances.

Cybersecurity Advisors

Cybersecurity advisors (CSAs) offer assistance with preparing and protecting private-sector entities and SLTT governments from cybersecurity threats. CSAs play an essential engagement and outreach role through their direct interactions with sector stakeholders affected by a cybersecurity incident. CSAs promote cybersecurity preparedness, risk mitigation, and incident response capabilities, working to engage stakeholders through partnership and direct assistance activities. CSAs work in coordination with regional offices for cybersecurity field operations.

Chemical Security Inspectors

Chemical Security Inspectors (CSIs) visit chemical facilities to ensure that they meet the security requirements set by the Chemical Facility Anti-Terrorism Standards (CFATS) program. CSIs conduct their visits according to data submitted to DHS by the facility in its Site Security Plan (SSP) or Alternative Security Program (ASP). The facility submits documentation to DHS that describes how it is meeting or plans to meet CFATS security standards, and the CSIs visit the facility to verify the accuracy of the submitted descriptions in comparison to the security measures present at the facility. CSIs also perform other visits and outreach activities as part of their mission to improve the security of chemical facilities

across the country. Through their visits, CSIs establish ties with local community stakeholders, such as law enforcement personnel and emergency first responders.

National Risk Management Center

The National Risk Management Center (NRMC) leads efforts to protect the Nation's critical infrastructure through an integrated analytical approach evaluating the potential consequences of disruption from physical or cyber threats and incidents. The results of this analysis inform decisions to strengthen infrastructure security and resilience, as well as response and recovery efforts during natural, man-made, or cyber incidents. NRMC uses all-hazards information from an array of partners to conduct consequence modeling, simulation, and analysis. NRMC's core functions include:

- Providing analytic support to DHS leadership, operational components, and field personnel during steady state and crises on emerging threats and incidents affecting the Nation's critical infrastructure.
- Assessing and informing national infrastructure risk management strategies on the likelihood and consequence of emerging and future risks.
- Developing and enhancing capabilities to support crisis action by identifying and prioritizing infrastructure through the use of analytic tools and modeling capabilities.

Appendix C. 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 infrastructure 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.

HSIN Connect

The HSIN Connect webinar tool is a robust conferencing tool, often used to disseminate priority information during an event. The tool provides a secure environment for real-time conferencing, web-based training, large-scale webinars, and real-time analysis and response. Various dashboards display up-to-date, relevant information about an event, along with best practices shared through HSIN Connect.

Sector-Specific Portals

Critical infrastructure sectors leverage sector-specific portals on HSIN-CI to provide situational awareness. These portals allow sector partners to effectively access and disseminate sensitive but unclassified information regarding topics and issues particular to their sectors among government and private-sector partners.

Joining HSIN

To support sector partner requests for access to HSIN and sector-specific portals, sector partners should send an email to HSIN.Outreach@hq.dhs.gov and include the following information:

- First and last name
- Valid email address
- Requested community of interest
- Reason for access

The community-of-interest validating authority reviews the membership application and approves or denies admission to the community of interest. If the application is approved, an email will be sent with instructions on how to log onto HSIN for the first time.

HSIN-CI and the sector-specific portals may be accessed through the [HSIN log-in webpage](#).

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





Appendix D. Information Security

Information security management is an essential part of information sharing. A best practice for agencies is to document when and how information should be shared with other entities. Information that is shared should clearly indicate the required level of safeguards and any restrictions on authorized access or use. The following are general examples of specific requirements for unclassified information:

- If the information contains personally identifiable information (PII), markings should comply with applicable regulations and guidelines. Organizations often require authorized recipients to complete related training and to agree to abide by the rules prior to receiving the information.
- If the information originated within the U.S. Department of Homeland Security (DHS) and is designated For Official Use Only (FOUO), the information must be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy. Distribution within DHS is on a need-to-know basis, with external dissemination requiring the authorization of the originator. For more information, see DHS Management Directive 11042.1, *Safeguarding Sensitive but Unclassified (For Official Use Only) Information*.
- If submitted by private-sector partners, the information may be marked as PCII, which assures private-sector partners that the government will not expose their sensitive or proprietary information and data to disclosure. To be designated as PCII, the information must be submitted to and approved by the PCII Program Office (PCII-Assist@hq.dhs.gov).

Traffic Light Protocol (TLP)

The Traffic Light Protocol (TLP) was created to facilitate greater sharing of information. TLP is a set of designations used to ensure that sensitive information is shared with the appropriate audience. The protocol employs four colors, each indicating the sharing boundaries the recipient(s) should apply. If the recipients need to share the information more widely than indicated by the original TLP designation, they must obtain explicit permission from the original source.

Color	When should it be used?	How may it be shared?
TLP: RED  Not for disclosure	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, TLP: RED information is limited to those present at the meeting. In most circumstances, TLP: RED should be exchanged verbally or in person.
TLP: AMBER  Limited disclosure	Sources may use TLP: AMBER when information requires support to be acted upon yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may share TLP: AMBER information only with members of their own organization and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources may specify additional intended limits of the sharing; recipients must adhere to the additional limits.
TLP: GREEN  Limited disclosure	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP: GREEN information may not be released outside of the community.
TLP: WHITE  Disclosure not limited	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Distribution is subject to the copyright guidance provided by the Office of the Chief Counsel. OCC should be consulted prior to the sharing of TLP: WHITE information.

Appendix E. Chemical Sector Partnership Council Member Organizations

Government Coordinating Council

U.S. Department of Commerce

Bureau of Industry and Security

U.S. Department of Homeland Security

Cybersecurity and Infrastructure Security
Agency, Infrastructure Security Division

Science and Technology Directorate

United States Coast Guard

U.S. Department of Justice

Federal Bureau of Investigation

Bureau of Alcohol, Tobacco, Firearms and
Explosives

U.S. Department of Transportation

Federal Motor Carrier Safety
Administration

Federal Railroad Administration

Pipeline and Hazardous Materials
Safety Administration

U.S. Environmental Protection Agency

Office of Emergency Management

Water Security Division

Sector Coordinating Council

Agricultural Retailers Association

American Chemistry Council

American Coatings Association

American Fuel and Petrochemical Manufacturers

Compressed Gas Association

Council of Producers & Distributors of
Agrotechnology

CropLife America

Institute of Makers of Explosives

International Institute of Ammonia
Refrigeration

International Liquid Terminals Association

Louisiana Chemical Association

National Association of Chemical Distributors

Society of Chemical Manufacturers and
Affiliates

The Chlorine Institute

The Fertilizer Institute

Appendix F. Incident Teleconferences

CISA conducts many of its incident management and coordination activities through outreach engagements that support information sharing with critical infrastructure stakeholders. The purpose of outreach engagements may be to provide information or recommendations to stakeholders and/or to collect information from stakeholders. Outreach engagements may be conducted under a variety of formats, including email, teleconferences, video teleconferences, and/or in-person meetings. For incidents affecting the sector, teleconferences are a primary mechanism for stakeholder outreach.

Incident-Specific Cross-Sector Calls

During significant incidents, the CIOCC will coordinate cross-sector calls to discuss national and cascading impacts and determine potential actions to mitigate risk. If necessary, the CIOCC may also conduct teleconferences at the regional level with locally affected partners, sharing information to enhance mutual situational awareness and address key areas of concern. Incident calls with private-sector stakeholders coordinated by the CIOCC are jointly held with the Federal Emergency Management Agency's National Business Emergency Operations Center.

National Threat Briefings

During periods of heightened threat or concern, the CIOCC may conduct unclassified teleconferences regarding current intelligence, expected actions, and protective measure options for consideration.

Sector-Specific Teleconferences

Sector-specific teleconference calls are intended to provide participants with a forum to share incident-specific information. The SSA management team is responsible for coordinating these teleconference calls.

The SSA management team coordinates with sector council leadership to determine an appropriate time for sector-specific teleconferences. The 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 entered into the national-level reporting system and reported out during cross-sector calls.

During sector-specific calls, personnel representing the SSA management team serve as moderators to structure the call and facilitate information exchange. The SSA personnel will also capture important information, identify key issues, and schedule follow-up conference calls.

Following the sector-specific call, the SSA management team will normally:

- Email a short recap of the sector-specific call to the sector councils.
- Send the CIOCC and CISA Crisis Action Team (CISA-CAT), as appropriate, any requests for information or assistance received during sector-specific calls.

In support of these teleconferences, the SSA management team may request information in advance from sector stakeholders, focusing on the following areas of interest:

- Primary sector-specific concerns or impacts
- Specific actions undertaken by key stakeholders
- Upcoming actions to be taken by key stakeholders
- Information needs and requests for assistance

Draft Agenda for Sector-Specific Teleconference

Objectives

- Provide situational awareness
- Discuss government and industry response activities
- Identify and discuss recovery priorities and limiting factors

Opening Comments and Roll Call

- SSA provides short status recap (from current CIOCC incident situation reports)

Government Update

- Federal Government activities
- State, local, tribal, and territorial (SLTT) activities
- Requests for information/assistance

Industry Update

- Industry-wide update (impacts across sector, general overview of impacted area, cascading impacts, response/recovery activities across sector)
- Impacted entity/entities (overview of the current situation from company perspective, status of response/recovery activities, estimates on response/recovery progress)
- Industry needs (requests for information/assistance, other needs)

Other Issues

Primary Point of Contact and Activation Status

- Emergency Operations Centers
- Fusion Centers
- SLTT Government Agencies
- Federal Joint Field Office
- Sector Contacts
- Regional Office

Call Schedule

Closing Comments

Adjourn

Secure Video Teleconferences

CISA and the Office of Intelligence and Analysis established quarterly or ad hoc secure video teleconferences (SVTCs) to exercise the ability of private-sector and SLTT partners—cleared under the DHS Private Sector Clearance Program or an SLTT clearance program—to locate and access a secure facility within their state or region to receive and view classified information at short notice or under exigent circumstances. The purposes of SVTCs are to:

- Exercise the ability to convene cleared private-sector partners in a classified space.
- Provide a general threat or situational awareness briefing to cleared private-sector participants.
- Facilitate collaboration and communication between local fusion centers, intelligence officials, protective security advisors, private-sector partners, and national sector council members.

Appendix G. Requests for Information and Requests for Assistance

Request for Information Procedures

The request for information (RFI) process is the formal procedure used to obtain information needed for assessment and analysis, product development, and decision support. RFIs provide specific and realistic information relevant to Cybersecurity and Infrastructure Security Agency (CISA) operations within a given timeframe.

The CISA Integrated Operations Coordination Center (CIOCC) provides personnel to serve in the role of an incident-specific RFI tracker. The RFI tracker coordinates responses to RFIs, tracks and monitors all RFI-related communications, and assists in generating near-real-time situational awareness and decision support products through all operational phases.

Upon receiving an RFI, the RFI tracker reviews the request to ensure the details (e.g., timelines, requestor information, and response requirements) are clear and sufficient before routing the RFI to the appropriate lead and secondary organizations for action. The RFI tracker assigns a tracking number to be used when referencing that specific RFI.

The CIOCC routes all RFIs within CISA before contacting any external agencies or organizations for information and/or assistance. If an external sector-specific agency (SSA) is the appropriate organization to provide a response to the RFI, that SSA serves as the lead organization for answering the RFI and may coordinate with CISA as a supporting organization to develop a response.

Request for Assistance Procedures

Critical infrastructure-related protection, response, and recovery activities operate within a framework of mutual aid and assistance. Incident-related requirements can be addressed through direct actions by owners and operators, or with government assistance provided by state, local, tribal, and territorial (SLTT) and/or federal authorities in certain circumstances.

Requests for assistance (RFAs) are received from critical infrastructure owners and operators or government partners seeking support for a variety of incident-related needs, including requirements for security, impact area access, fuel, or accommodations for crews needed to perform work for repair/restoration of critical services. Generally, SLTT authorities, SSAs, National Response Framework Emergency Support Function (ESF) primary or supporting agencies, or other Federal Government entities provide primary entry points for these requests.

- Critical infrastructure partners affected by an event should first attempt to submit RFAs through the local SLTT emergency agency. To ensure awareness at the national level, owners/operators may also submit such RFAs to the CIOCC per the contact information provided in this playbook's supplemental Contact Information and inform the CIOCC of other submissions.
- Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) members may also send RFAs to the CIOCC or through the SSA management team.
- The CIOCC maintains an automated master log of all RFAs submitted for action and is responsible for tracking all RFA submissions through task completion.
- The SSA management team should address significant an outstanding RFA if the issue requires immediate attention; for less urgent matters, the SSA management team may collaborate with the GCC and SCC leadership during a sector teleconference call.

For information on RFI and RFA forms, contact ciocc@cisa.dhs.gov or (202) 282-9201.

Appendix H. Regulatory Waivers

Appropriate federal, state, local, tribal, or territorial government entities may receive requests from sector owners and operators on waivers for regulatory or legal requirements for incident response. Considerations in waiver assessment can include determining which government entities have the authority, what information would be needed from requesting owners and operators, how requests would be made, and expected timelines. Not all regulatory or other legal requirements can be waived. The following are key resources for regulatory waivers.

Surface Transportation

Federal Motor Carrier Safety Regulation Waivers

Exemptions (“waivers”) from many of the Federal Motor Carrier Safety Regulations occur “automatically” in accordance with 49 CFR [Code of Federal Regulations] 390.23 when the President of the United States, a state governor, or a local government official issues a declaration of emergency (as defined in 49 CFR 390.5). Presidential and state declarations are effective for up to 30 days, and local declarations are effective for up to 5 days. Only a Federal Motor Carrier Safety Administration (FMCSA) field administrator or regional field administrator has authority to extend the waivers beyond the initial 30 days and to place additional restrictions on the waivers.

The waivers apply to any commercial motor vehicle responding from anywhere in the United States to provide direct relief to the emergency. Emergency declarations temporarily lift most safety regulations, including hours of service, from interstate motor carrier drivers and operators providing emergency relief.

Utility service vehicles are always exempt from hours-of-service limitations when they are providing for the operating, repairing, and maintaining of public utilities. Government vehicles are always exempt, but government contractors are not (unless an emergency declaration is in effect).

The FMCSA provides additional information at www.fmcsa.dot.gov/emergency and has established a toll-free hotline number at 1-877-831-2250 for anyone seeking inquiries pertaining to FMCSA regulations during a declared disaster.

Federal Motor Carrier Waivers

Regulatory parts of 49 CFR that can be lifted are from 390–399, most significantly:

- 390: General Requirements (e.g., recordkeeping, vehicle marking)
- 391: Driver Qualifications (e.g., physical standards, English language proficiency)
- 392: Driving of Commercial Motor Vehicles (e.g., pre-trip inspection, fatigued operation)
- 393: Parts and Accessories (e.g., lighting, cargo securement)
- 395: Hours of Service (e.g., 11-hour driving limit, 14-hour on-duty limit)
- 396: Inspection, Repair and Maintenance (e.g., post-trip and annual trip inspections)

The following are not exempt: drug and alcohol testing, commercial driver’s license requirements, insurance requirements, hazardous materials regulations, state vehicle registration requirements, consumer protection regulations for household goods movers, and other federal commercial regulations.

Divisible Load Permits

During an emergency, states may issue special divisible load permits to overweight vehicles and loads that can easily be dismantled or divided if all of the following conditions are met:

- The President has declared an emergency or a major disaster under the Stafford Act.
- The permits are issued in accordance with state law.
- The permits are issued exclusively to vehicles and loads that are delivering relief supplies.

More information on divisible loads and the Fixing America's Surface Transportation (FAST) Act is available at www.fhwa.dot.gov/fastact/factsheets/trucksizeweightfs.cfm.

Oversize/Overweight Freight Permits

The federal maximum size/weight requirements are 80,000 gross, 20,000 single-axle, 34,000 tandem, and bridge formula. It is the responsibility of the motor carrier to ensure that the permits being requested are appropriate for the states being traversed. To obtain oversize/overweight permits, the state(s) in which the vehicles will travel will need to be contacted. For information on state permitting offices, visit http://ops.fhwa.dot.gov/freight/sw/permit_report/index.htm.

During a state of emergency declaration, states normally put a process in place to expedite the permitting process. Section 1511 of the Moving Ahead for Progress in the 21st Century Act (MAP-21), amending 23 U.S.C. § 127, extends the states' authority to issue special permits to vehicles with divisible loads that are delivering relief supplies during emergency and disaster responses. In addition, some states have special legislative or "grandfather" provisions that allow additional weight for interstate travel. On a case-by-case basis, a list of states with "grandfather" provisions can be made available. Special permits issued under Section 1511 of MAP-21 expire not later than 120 days after the date on which the President declares an emergency to be a major disaster.

State-Specific Waivers Needed to Transport Restoration Vehicles Interstate

Weight Limits: 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, so limits differ from state to state. States may waive their typical weight limits and set temporary limits for trucks carrying emergency relief supplies to allow rapid movement of the largest amount of resources that can be moved safely intrastate and across state lines. A typical waiver may allow trucks weighing from 92,000 lbs. to 100,000 lbs.

Hours of Service: Some states have driver hours-of-service requirements that are more restrictive than those of the U.S. Department of Transportation (DOT). Such states may waive those requirements, in coordination with DOT, to get as many resources into the disaster area as possible in a short amount of time.

Toll Waivers

Toll waivers are granted on a case-by-case basis during emergency and disaster assistance. This is up to each individual state and/or toll authority. If toll waivers are not granted, receiving precise directions on how restoration crews/fleets should transit through tolls is also a key consideration.

Truck/Weigh Station Bypass

States can make a judgment call to allow certain vehicles to bypass the truck/weigh stations based on the configurations of known vehicles during emergency and disaster response.

Railroads

Federal Railroad Administration Emergency Relief Docket

Federal Railroad Administration Emergency Relief Dockets (FRA ERDs), which are designed to provide temporary, expedited waiver relief from railroad safety regulations in certain emergency situations, may play an important role in the emergency movement of heavy equipment by the Chemical Sector.

Pursuant to 49 CFR 211.45, the FRA administrator may designate specific events (e.g., hurricanes and severe winter storms) as emergencies that trigger the opening of an FRA ERD. Once the ERD is opened, railroads may submit emergency requests for regulatory waivers to the docket. FRA's Railroad Safety Board may then give these waiver requests expedited review and, if merited, without prior notice and comment.

Aviation

Commercial Unmanned Aircraft Systems Operations

Sectors may utilize unmanned aircraft systems (UASs) in their operations for damage assessments following an incident. During an emergency, the Federal Aviation Administration (FAA) may issue flight restrictions in the vicinity of disaster areas, as response operations may involve authorized aircraft flying at very low altitudes over affected areas. Unauthorized UAS operations may prevent other aircraft from performing life-saving missions and increase the risk of mid-air collision. The FAA must approve UAS operators supporting disaster response operations before UAS flights begin.

Operators may seek approval by following these steps:

- The operation must contribute directly to the response, relief, or recovery effort.
- The operator must secure support from a governmental entity.
- After obtaining government advocacy, the operator must contact the FAA's Systems Operations Support Center (SOSC) at 202-267-8276 for assistance.
- After calling the SOSC, the operator must submit the request via email to 9-ator-hq-sosc@faa.gov.

Appendix I. National-Level Reporting

In support of national-level reporting (NLR) requirements, the CISA Integrated Operations Coordination Center (CIOCC) will serve as the overall federal focal point for critical infrastructure-related status reporting from the sector-specific agencies (SSAs), government coordinating councils (GCCs), sector coordinating councils (SCCs), owners and operators, and other information-sharing entities. When directed by the CIOCC, the SSA management team must report on impacts to the sector from an incident, entering the information into the NLR system. The CIOCC uses information incorporated into the NLR system to prepare situation reports, which are provided to senior levels in government, GCCs, SCCs, and owners/operators via the Homeland Security Information Network (HSIN).

The following actions occur when NLR begins:

- The CIOCC alerts SSAs that the reporting process has begun via email notification or other means transmitted from the CIOCC Watch and Warning. SSAs then coordinate with SCCs, GCCs, and established information-sharing and analysis mechanisms in their sectors to initiate status reporting and impact assessments.
- The CIOCC verifies reported information and compiles the critical infrastructure situation report, which is included in the National Common Operating Picture posted to HSIN – Critical Infrastructure (HSIN-CI).
- SSAs are responsible for notifying the CIOCC when they receive additional event-related information from within their sectors. The CIOCC documents these reports, compiles additional details surrounding the incident, and disseminates reports to the sectors, the National Operations Center, National Response Coordination Center, National Risk Management Center, and Federal Bureau of Investigation.

Information Required for National-Level Reporting

When directed by the CIOCC to begin NLR, the SSA management team provides the following information:

- 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

Collaboration with Sector Partners

To complete the information required by NLR, the SSA management team will reach out to sector partners to request information regarding sector-level impacts and corresponding prevention, protection, mitigation, response, and recovery actions. The types of information requested include:

- Impacts to nationally significant critical infrastructure
- Impacts to regionally significant critical infrastructure
- Cross-sector impacts within the incident area

- Dependencies, interdependencies, and cascading effects on critical infrastructure beyond the immediate incident area and directly affected critical infrastructure sectors
- Critical foreign dependencies (assets) affected by the incident
- Actions required by sectors and agencies beyond those needed for infrastructure restoration within the incident area

Report Collected Information

The SSA management team reports this information to the CIOCC via the NLR tool, to the Cybersecurity and Infrastructure Security Agency's Crisis Action Team, and to the SCC leadership, as appropriate.

Appendix J. Authorities

Defense Production Act, Public Law 81-744. <http://www.gpo.gov/fdsys/pkg/PLAW-111publ67/html/PLAW-111publ67.htm>.

Federal Emergency Management Agency (FEMA), Presidential Policy Directive 40, National Continuity Programs, Washington, D.C. June 21, 2017. <https://www.fema.gov/national-continuity-programs>.

Homeland Security Act of 2002, Public Law 107-296, as amended. <https://legcounsel.house.gov/Comps/Homeland%20Security%20Act%20of%202002.pdf>.

Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act), Public Law 93-288. http://www.fema.gov/pdf/about/stafford_act.pdf.

The White House, Executive Order 13636, Improving Critical Infrastructure Cybersecurity, Washington, D.C. February 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

The White House, Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, Washington, D.C. February 13, 2015. <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari>.

The White House, Homeland Security Presidential Directive 5, Management of Domestic Incidents, Washington, D.C. February 28, 2003. <https://www.dhs.gov/publication/homeland-security-presidential-directive-5>.

The White House, Presidential Policy Directive 8, National Preparedness, Washington, D.C. March 30, 2011. <http://www.dhs.gov/presidential-policy-directive-8-national-preparedness>.

The White House, Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, Washington, D.C. February 12, 2013. <http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

The White House, Presidential Policy Directive 41, United States Cyber Incident Coordination, Washington, D.C. July 26, 2016. <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident>.

U.S. Department of Homeland Security, Federal Emergency Management Agency, National Disaster Recovery Framework (Second Edition), Washington, D.C. September 2011. <http://www.fema.gov/national-disaster-recovery-framework>.

U.S. Department of Homeland Security, Federal Emergency Management Agency, National Response Framework (Second Edition), Washington, D.C. May 2013. <http://www.fema.gov/national-response-framework>.

U.S. Department of Homeland Security, Federal Emergency Management Agency, Critical Infrastructure and Key Resources Support Annex to the National Response Framework, Washington, D.C. May 2013. <http://www.fema.gov/media-library/assets/documents/32261?id=7386>.

U.S. Department of Homeland Security, Office of Infrastructure Protection, Incident Management Base Plan, Washington, D.C. 2009.