

Coordinating Agency:

Department of Homeland Security

Cooperating Agencies:

All

INTRODUCTION

Purpose

This annex describes the policies, responsibilities, and concept of operations for Federal incident management activities involving the private sector during incidents requiring a coordinated Federal response. In this context, the annex further describes the activities necessary to ensure effective coordination and integration with the private sector, both for-profit and not-for-profit, including the Nation's critical infrastructure, key resources, other business and industry components, and not-for-profit organizations (sometimes called nongovernmental organizations (NGOs)), including those serving special needs populations, engaged in response and recovery. The Critical Infrastructure and Key Resources (CIKR) Support Annex focuses on the CIKR efforts of the private sector while this annex focuses on the remaining portion of the private sector.

Scope

This annex applies to all Federal executive agencies operating under the *National Response Framework (NRF)* in incidents requiring a coordinated Federal response that involve the private sector in any of the following ways:

- Impacted organization or infrastructure¹
- Response resource
- Regulated and/or responsible party
- Member of the State emergency management organization

Chapter I of the *NRF* core document describes the private-sector role in incident management activities. This annex addresses those aspects of incident management regarding the private sector that must be emphasized because of their uniqueness or importance.

This annex does not alter existing private-sector responsibilities for emergency management under the law. Existing contractual or other legal relationships between Federal agencies and the private sector are not supplanted by this annex.

The CIKR efforts involve a wide array of public and private incident managers and CIKR security partners within immediate incident areas as well as at regional and national levels. The CIKR Support Annex details the roles and relationships between the private sector and the Federal Government for CIKR.

The roles and interfaces of voluntary and other not-for-profit organizations and linkages of potential donors of goods and services to governments and NGOs are detailed in the Volunteer and Donations Management Support Annex and the Emergency Support Function (ESF) #6 – Mass Care, Emergency Assistance, Housing, and Human Services Annex.

¹...that falls within the definition of critical infrastructure and key resource (CIKR), as described in Homeland Security Presidential Directive (HSPD) 7, "Critical Infrastructure Identification, Prioritization, and Protection," and as they relate to the *NRF*.

The roles of Sector-Specific Agencies (SSAs), as defined in Homeland Security Presidential Directive (HSPD) 7, are addressed in more detail in the CIKR Support Annex.

Detailed processes, procedures, and protocols for incident management coordination with the private sector are developed and promulgated separately by the Department of Homeland Security (DHS).

Policies

The Federal Government encourages cooperative relations between private-sector organizations and State, tribal, and local authorities regarding prevention, preparedness, mitigation, response, and recovery activities. Active public-private sector coordination and cooperation through the emergency management cycle, beginning with planning, is a best practice recommendation common to the *National Incident Management System (NIMS)*, the Standard of the Emergency Management Accreditation Program (EMAP), and for the private sector, the National Fire Prevention Association (NFPA) 1600 Standard for Disaster/Emergency Management and Business Continuity Programs.

Since the release of the 9/11 Commission Final Report and the passage of the Intelligence Reform Act of 2004, DHS has worked with the private sector to articulate the mutual benefits and foster implementation of the NFPA 1600. Pursuant to the 9/11 Commission Act of 2007, DHS will develop and promote a preparedness program for private-sector entities that voluntarily choose to seek certification. DHS also is supporting the development and updating of voluntary preparedness standards. A private-sector firm that complies with their appropriate standards will benefit from its compliance both in its preparedness and its ability to promote public awareness of its compliance.

The Federal Government encourages processes that support informed cooperative decisionmaking. It takes actions that engage the private sector at the strategic (e.g., chief executive officer (CEO), corporate president, or other senior leadership, etc.) and operational levels to ensure:

- Effective and efficient use of private-sector and Federal resources.
- Timely exchange of information.
- Public and market confidence in times of crisis or catastrophe.

The Federal Government encourages extensive two-way and multidirectional sharing between the public and private sectors of operational information and situational awareness relative to potential or actual incidents. The Federal Government works cooperatively to develop and apply processes, procedures, and communications protocols that support such sharing at the strategic leadership and operational levels. A few examples of such information sharing are: (1) Homeland Security Information Network-Critical Sectors (HSIN-CS); (2) TRIPwire program, which provides situational awareness on improvised explosive devices; and (3) National Coordinating Center (NCC) for Telecommunications daily communications.

The Federal Government encourages members of the CIKR community to organize sector-coordinating and information-sharing mechanisms suitable for their sectors or areas of concern.

The Federal Government encourages owners and operators of those infrastructure elements whose disruption may have national or regional impact to develop appropriate emergency response plans and information-sharing processes and protocols tailored to the unique requirements of their respective sectors or industries, and mapped clearly to regional, State, tribal, and local emergency response plans and information-sharing networks.

The Federal Government encourages private-sector organizations to develop and maintain capabilities needed to respond to and manage a complete spectrum of incidents and emergencies, except in cases where the capabilities are inherently governmental in nature.

In certain circumstances, Federal law requires appropriate authorities to include private-sector representatives in incident management planning, operations, and exercises; when not required, it encourages such participation whenever practical.

The Federal Government may direct private-sector response resources in some cases in which contractual relationships exist. The Government also retains its full authorities to oversee and control as appropriate infrastructure involved in an incident. Through the Defense Production Act² and the Homeland Security Act, DHS has the authority to redirect production and distribution of certain incident management resources, if required.

The Federal Government treats information provided by the private sector, from receipt through destruction, in a manner consistent with applicable statutes and regulations. These handling procedures include Protected Critical Infrastructure Information, providing exemption from disclosure, to protect from unauthorized disclosure appropriately designated proprietary or otherwise sensitive company information.

The Federal Government avoids actions that disrupt existing relationships between voluntary aid providers at the local, tribal, State, or national level when eliciting additional offers of goods and services.

The Federal Government conducts after-action critiques of the procedures detailed in this annex with private-sector participants when they are practiced in national-level, DHS-sponsored exercises; it shares such critiques appropriately with private-sector participants.

The Federal Government supports measures that ensure site accessibility for essential services providers responding to disasters or emergencies. Essential services providers, as defined in the Stafford Act as amended by Public Law 109-347, include: "(a) a municipal entity; (b) a nonprofit entity; or (c) a private, for-profit entity" that contributes to efforts to respond to an emergency or major disaster. These entities provide:

- Telecommunications service;
- Electrical power;
- Natural gas;
- Water and sewer services; or
- Any other essential service, as determined by the President.

CONCEPT OF OPERATIONS

General

The operational concept for incident management involving the private sector is the concept specified in the *NRF* and the *NIMS*.

² See the Defense Production Act of 1950, as amended, as referenced in the section on private sector roles and responsibilities in the *NRF* core document.

The concept of operations in this annex covers the specific organizations and actions developed that are required to effectively and efficiently integrate incident management operations with the private sector. These are detailed in the sections that follow.

Organizations for Operations With the Private Sector

General: Specialized organizations that facilitate coordination with the private sector are designed to provide for critical needs as listed below:

- Processes to determine the impact of an incident on the sector involved, as well as to forecast cascading effects of interdependencies between sectors.
- Procedures for communication that facilitate a shared situational awareness across industry and infrastructure sectors and between the public and private sectors, including individuals with special needs.
- Procedures for coordination and priority-setting for incident management support and response, and the rationing or prioritizing of the delivery of goods and services after an incident.
- Processes to inform Federal Government decisionmakers to help determine appropriate recovery and reconstitution measures, particularly in cases where they may result in indemnity, liability, or business losses for the private sector.
- Procedures for the Federal Government to obtain, under the Defense Procurement Act and other authorities, goods and services necessary for the restoration and recovery of CIKR and other key elements of the economy on a priority basis.

Department of Homeland Security: In the event of a potential or actual incident, the DHS Office of the Secretary coordinates strategic communications with CEOs, senior officials, or individuals specifically designated by these private-sector leaders to engage in such communications on their behalf.

Further, the Secretary of Homeland Security utilizes a private-sector advisory group with representatives from across the spectrum of CIKR, business, and industry, as well as not-for-profit organizations, to provide advice on incident management and emergency response issues affecting their constituencies.

The Office of the Secretary assigns the responsibility for private-sector threat or incident communications to appropriate organizations within DHS. These organizations are detailed below.

- **Private Sector Office (DHS/PSO):** The DHS/PSO encourages private-sector preparedness for incident management by:
 - Identifying and promoting security and preparedness activities in national preparedness, prevention, response, and recovery.
 - Promoting educational efforts to prepare for natural disasters or terrorist incidents.
 - Encouraging the identification and sharing of best practices through promoting use of consensus standards and best practices.

DHS/PSO provides representatives to the National Operations Center (NOC) components as required, and to the Joint Field Office (JFO) to enable strategic coordination with the private sector during incidents requiring a coordinated Federal response.

- **Office of Infrastructure Protection (DHS/OIP):** DHS/OIP supports prevention, preparedness, response, and recovery efforts involving CIKR, in accordance with HSPD-7, and other private-sector entities as appropriate, through facilitating and coordinating protection and response planning, procedures, and exercises. DHS/OIP implements the programmatic policy and strategy for information sharing.

DHS/OIP is responsible for the implementation and ongoing management and maintenance of the *National Infrastructure Protection Plan (NIPP)*. The *NIPP*, and its associated CIKR Sector-Specific Plans (SSPs), work in conjunction with the *NRF* and its supporting annexes to provide a foundation for CIKR preparedness, protection, response, and recovery efforts in an all-hazards context.

As noted above, the CIKR Support Annex provides the authoritative and more comprehensive discussion of the policies and concept of operations for assessing, prioritizing, protecting, and restoring CIKR during incidents.

Day-to-day public-private coordination structures, information-sharing networks, and risk management frameworks used to implement *NIPP* steady-state CIKR protection efforts continue to function and provide coordination and support for CIKR protection and restoration for incident management activities under the *NRF*.

The *NIPP* establishes the overall risk-based construct that defines the unified approach to protecting the Nation's CIKR in an all-hazards context, and specifies procedures and activities to reduce risk to the Nation's CIKR on a day-to-day basis, including:

- The sector partnership model that encourages use of Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), and cross-sector coordinating councils to create an integrated national infrastructure protection framework for CIKR protection and restoration across sectors.
- The networked approach to CIKR information sharing that provides for multidirectional CIKR-related exchanges of actionable intelligence, alerts and warnings, best practices, and other matters between and among various nodes including: Federal CIKR Sectors; State, tribal, and local entities; the Intelligence Community; law enforcement; and CIKR owners and operators.

The "value proposition" set forth in the *NIPP* articulates guiding principles for coordination and cooperation between government and the CIKR sector. In accordance with these principles, the Federal Government:

- Provides CIKR owners and operators timely, accurate, and actionable all-hazards information.
- Ensures CIKR owners and operators are engaged at senior executive and operational levels primarily through respective SCCs.
- Articulates benefits of a risk-based, cross-sector approach to preparedness, resilience, and protection.
- Works with CIKR owners and operators to clearly establish priorities for prevention, protection, and recovery.
- Articulates the mutual benefits of all-hazards preparedness to Federal, State, tribal, and local governments as well as to CIKR owners and operators, thereby underscoring the importance of private-sector participation in preparedness, prevention, response, and recovery efforts. (See the CIKR Support Annex for more information on the value proposition for private-sector action.)

Key DHS/OIP functions that support coordination with CIKR private-sector entities for incident management include:

- Facilitating information sharing and situational awareness with security partners.
- Facilitating coordination of a sector partnership model that fosters cooperation and collaboration between government and private-sector owners and operators within each of the 17 CIKR Sectors.
- Facilitating the development, implementation, and exercise of CIKR support as an integrated element of response plans across sectors, and other industry sectors as appropriate.
- Supporting sectors in developing their own sector coordination and information-sharing mechanisms.
- Deploying Infrastructure Liaisons to the NOC components including the National Response Coordination Center (NRCC) and the Interagency Management Planning Team (IMPT) to facilitate coordination with the CIKR sectors at the national level.
- Deploying Infrastructure Liaisons and/or Advisors (Specialists) as requested to the Regional Response Coordination Center (RRCC), JFOs and other field facilities, and State, tribal, or local emergency operations centers, as needed, to provide coordination and liaison functions to the CIKR sectors.

Although the role of the Infrastructure Liaison is comprehensively described in the CIKR Support Annex, high-level responsibilities can be found below.

- Serves as the principal advisor regarding national and regional CIKR, and other relevant businesses and industry.
- Coordinates with private-sector entities, SSAs, and State, tribal, and local governments.
- Acts as liaison between national- and regional-level CIKR, the private sector, and the Unified Coordination Group by conveying information about the Nation's CIKR and private-sector status.
- Facilitates operational-level communication with the private sector during an incident.
- Communicates with the DHS/OIP representative at the IMPT, NRCC, and National Infrastructure Coordinating Center (NICC).

The Infrastructure Liaison focuses on the broad impacts and status of actions relating to affected CIKR, as opposed to the direct provision of goods or services.

Restoration of critical infrastructure and operational coordination with impacted telecommunications, energy, and other utilities and systems is conducted through the established ESFs.

- **National Infrastructure Coordinating Center (NICC):** The NICC monitors the Nation's CIKR on a 24/7 basis and provides a mechanism and process to share and exchange information with the private sector and the HSPD-7 SSAs.

In incidents requiring a coordinated Federal response, the NICC is a key component in providing situational and operational awareness and the capability to rapidly share information with private-sector entities as required.

Sector-Specific Agencies

SSAs, as designated in HSPD-7, focus on overarching CIKR protection, risk management, and information sharing by working collaboratively with relevant Federal departments and agencies; State, tribal, and local governments; CIKR owners and operators; and other private-sector entities.

In cooperation with DHS/OIP, SSAs collaborate with private-sector security partners to encourage:

- Supporting comprehensive risk assessment/management programs for high-risk CIKR.
- Sharing real-time incident notification, as well as CIKR protection best practices and processes.
- Developing information-sharing and analysis mechanisms to include physical and cyber threats.
- Building security-related information sharing among public and private entities.

Private-Sector Involvement With Incident Management Organizations: Private-sector involvement with incident management organizations is determined by the nature, scope, and magnitude of the incident.

Private-Sector Incident Management Organizations: Private entities such as businesses and industry associations develop, validate, exercise, and implement security and business continuity plans to ensure their capability to deliver goods and services. Assessments of, and contingency plans for, the disruption of a private entity's supply chain and other dependencies are usually included in this planning.

Private-sector owners and operators, in many locations, coordinate plans for security and continuity/contingency programs with State, tribal, and local entities.

In accordance with the *NIPP*, CIKR sectors use established information-sharing arrangements to facilitate coordination necessary to share homeland security information with competitors and governments.

Representative private-sector incident management organizations may be established to assist Federal, State, tribal, or local regional-level or local coordination centers or field offices to facilitate interaction, communication, and coordination with the private sector.

State and Local Incident Management Organizations: Many States coordinate across regions to support various response activities. Their incident management organizations act as conduits for requests for Federal assistance when an incident exceeds local and private-sector capabilities.

Private-sector organizations, either for-profit or not-for-profit, may be included in the Incident Command Post.

Federal Incident Management Organizations: Private-sector for-profit and not-for profit organizations, as well as State, tribal, local, and NGOs are encouraged to assign liaisons to the JFO to facilitate interaction, communication, and coordination. In some instances, the Unified Coordination Group may include not-for-profit and/or for-profit organization representatives.

Notification and Reporting

Private-sector for-profit and not-for-profit organizations, like Federal, State, tribal, and local governmental organizations, report threats, incidents, and potential incidents to the NOC using existing jurisdictional incident reporting mechanisms and reporting channels. The NOC receives threat and operational information regarding incidents or potential incidents from these organizations and jurisdictions and makes an initial determination to initiate the coordination of Federal incident management activities.

In partnership with the NOC, the DHS/OIP manages the daily analysis of incident-related reports and information. This management includes maintaining communications with private-sector critical infrastructure information-sharing mechanisms.

During national-level incidents that require Federal coordination, the NICC conducts daily teleconferences with the CIKR sector information-sharing mechanisms and SSAs to discuss incident-related activities and sector status.

CIKR Incident-Related Communication: The DHS Office of Public Affairs (DHS/OPA) works in conjunction with DHS/OIP and the DHS Assistant Secretary for the Private Sector providing timely public information to the CIKR sectors and their affiliated entities (through conference call, e-mail, or both) during national-level incidents that require a coordinated Federal response.

The CIKR incident communications system is modeled after processes set forth in the *NRF* Public Affairs Support Annex to ensure coordination with Federal, State, tribal, and local entities.

DHS/OPA communication actions include the following:

- Providing the overarching coordination lead for incident communications to the public, including the special needs population, during an incident requiring a coordinated Federal response.
- Maintaining a standing conference line for use by CIKR incident communications coordinators.
- Coordinating and disseminating line access information in coordination with DHS/OIP.
- Maintaining a contact list, including e-mail information, of CIKR incident communications coordinators.
- Coordinating with SSAs to share public information and messages for SCCs.

DHS/PA works in coordination with ESFs and SSAs to identify organizations and/or individuals (e.g., SCCs, sector-identified information-sharing mechanisms such as Information Sharing and Analysis Centers (ISACs), major trade associations and other private-sector organizations as appropriate, and State, tribal, and local entities) to act as focal points for incident communications with the private sector. These organizations and individuals are selected based on their ability to disseminate information to and coordinate with a broad array of other organizations and individuals.

Representatives serve as the primary reception and transmission points for incident communications products from DHS/PA, ESFs, and SSAs, and they retain responsibility for dissemination to counterpart communicators to ensure information is distributed widely.

ACTIONS RELATED TO OPERATIONS WITH THE PRIVATE SECTOR

Preincident

DHS/PSO facilitates the development and presentation of general educational programs for the private sector that increase awareness and understanding of terrorist threats and prevention and mitigation activities, encourages the sharing of appropriate information and use of best practices that contribute to early warning of potential incidents, and supports private-sector participation in exercises.

DHS/OIP facilitates and encourages the organization of industry sectors to cooperate on information sharing and other prevention and mitigation activities.

DHS/OIP maintains relationships with the CIKR sector to identify requirements for capabilities and support. DHS/OIP develops and implements programs and capabilities that continuously improve the two-way exchange of information with the private sector.

DHS/OIP maintains situational/operational awareness of CIKR through the NICC working in conjunction with the information-sharing mechanisms. It assesses the data it receives to identify anomalies in sector operations, working closely with CIKR owners and operators. After assessing information on incidents and threats, it disseminates alerts, warnings, and advisories for both government and private-sector entities.

DHS/OIP, in collaboration with SSAs, encourages, facilitates, and coordinates CIKR and other industry sectors to develop and implement industry best practices for preparedness, perform sector-wide preparedness planning and implementation, plan coordination with regional and local government plans, and perform cross-sector integration of plans.

DHS/OIP supports sector-specific and cross-sector exercises and provides representation in exercises led by the private sector and State, tribal, and local governments.

Initial Actions

Actions are initiated at DHS Headquarters, the NOC, the NRCC, the NICC, and RRCCs to facilitate coordination with relevant private-sector entities.

The ESFs also implement established protocols for coordination with private-sector counterparts at the national and regional levels. To facilitate private-sector coordination, DHS assigns representatives to the various *NRF* organizational structures.

The DHS/PSO representatives act as a liaison to communicate at a strategic level to private-sector leadership. DHS/PSO facilitates communication with private-sector senior leadership and with the NRCC and NICC to maintain awareness of private-sector issues and needs as a complement to awareness being achieved by DHS/OIP. They also coordinate the incident's economic impact assessment with private-sector senior leaders, internal DHS partners, and other Federal department or agency liaisons as appropriate.

At the NOC Watch, the DHS/OIP representative monitors the operational status of CIKR and facilitates coordination and sharing of situational awareness with and among the CIKR and other industrial sectors as needed.

The NICC coordinates between the owners and operators of CIKR and other private assets, and the appropriate SSAs, to ensure that all are informed regarding activities pertaining to their areas of responsibility. SSAs coordinate with the NICC to ensure that it is informed regarding CIKR vulnerabilities and activities and in support of the DHS common operating picture.

The Infrastructure Liaison at the JFO facilitates coordination between the Unified Coordination Group, and Principal Federal Official, if appointed, with the national-level *NRF* elements and appropriate ESF representatives regarding local/regional matters relating to CIKR and the private sector.

The Infrastructure Liaison provides analysis and recommendations to the Unified Coordination Group regarding restoration of the infrastructure and related allocation and prioritization of limited resources. (See the CIKR Support Annex for further discussion of Infrastructure Liaison roles and responsibilities.)

Emergency Support Functions: At the NRCC, RRCC, and JFO, the ESFs establish contact with private-sector counterpart organizations and/or industry, including representative private-sector organizations created for such incident to assist in assessment of impacts and identification of resources available to support potential or actual incident management efforts.

In some circumstances, priorities of incident management actions are developed by a partnership of Federal, State, and private-sector entities.

Ongoing Actions

Private-sector entities are responsible for the repair, restoration, and security of their property, and first seek reimbursement for disaster losses from insurance or other sources.

Federal disaster assistance may be available, primarily in the form of low-interest disaster loans from the U.S. Small Business Administration.

DHS/PSO and other DHS entities, as assigned, assist and facilitate private-sector relationships with DHS as they implement recovery plans and return to normal operations.

The NICC maintains situational awareness through the recovery of CIKR and acts as a conduit of information to and from sectors through the NICC.

DHS/OIP assists or facilitates infrastructure owners and operators with the restoration of facilities, working under existing authorities, in coordination with private-sector organizations and consortia that are organized for these purposes.

RESPONSIBILITIES

Coordinating Agency: DHS

DHS:

- Develops plans, processes, and relationships, and facilitates coordinated response planning with the private sector at the strategic, operational, and tactical levels.
- Shares information, including threats and warnings, before, during, and after an incident.
- Informs and orients the private sector on the contents of the *NRF*, and encourages and facilitates the development and coordination of equivalent private-sector planning.
- Coordinates and conducts national and regional incident management functions with the private sector and State, tribal, and local governments.
- Develops, implements, and operates information-sharing and communication strategies, processes, and systems with homeland security stakeholders.

Cooperating Agencies

The primary agency(ies) for each ESF is responsible for developing and maintaining working relations with its associated private-sector counterparts through partnership committees or other means (e.g., ESF #2 – Communications: telecommunications industry; ESF #10 – Oil and Hazardous Materials Response: oil and hazardous materials industry; etc.).

Private-Sector Entities

Private-sector organizations support the *NRF* either through voluntary actions to help ensure business continuity or by complying with applicable laws and regulations.

To assist in response and recovery from an incident, private-sector organizations:

- Take responsibility for their internal preparedness by:
 - Identifying risks, performing vulnerability assessments.
 - Developing contingency and response plans.
 - Enhancing their overall readiness.
 - Implementing appropriate prevention and protection programs.
 - Coordinating with their suppliers and CIKR customers to identify and manage potential cascading effects of incident-related disruption through contingency planning.
- Accept responsibility to:
 - Share information appropriate within the law with the government.
 - Provide goods and services through contractual arrangements or government purchases, or and where appropriate, mutual aid and assistance agreements with host communities.
 - Act as corporate citizens to donate and facilitate donations by others of goods and services.
 - Certain organizations are required to bear the cost of planning and response to incidents, regardless of cause. When requested by DHS, these private-sector organizations are expected to mobilize and employ the resources necessary and available in accordance with their plans to address the consequences of incidents at their own facilities or incidents for which they are otherwise responsible.

This page intentionally left blank.