Coordinating Agency:

Department of Homeland Security

Cooperating Agencies/Organizations:

Department of Agriculture
Department of Commerce
Department of Defense
Department of Education
Department of Energy
Department of Health and Human Services
Department of the Interior
Department of Justice
Department of Labor
Department of State
Department of Transportation
Department of the Treasury
Department of Veterans Affairs
Environmental Protection Agency
Federal Energy Regulatory Commission
Intelligence Community
Nuclear Regulatory Commission
Office of Science and Technology Policy
U.S. Postal Service
Information Sharing and Analysis Center Council
Partnership for Critical Infrastructure Security
State, Local, Tribal, and Territorial Government Coordinating Council

INTRODUCTION

Purpose

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

- Describes roles and responsibilities for CIKR preparedness, protection, response, recovery, restoration, and continuity of operations relative to *National Response Framework (NRF)* coordinating structures and *National Incident Management System (NIMS)* guiding principles.

- Establishes a concept of operations for incident-related CIKR preparedness, protection, response, recovery, and restoration.[1]

- Outlines incident-related actions (including preresponse and postresponse) to expedite information sharing and analysis of actual or potential impacts to CIKR and facilitate requests for assistance and information from public- and private-sector partners.

[1] Restoration is an element of recovery and, within the context of this annex, is defined as returning CIKR services and site performance capabilities.

Scope

This annex addresses integration of the CIKR protection[2] and restoration mission as a vital component of the Nation's unified approach to domestic incident management, which also may include CIKR-related international considerations.

Critical infrastructure includes those assets, systems, networks, and functions—physical or virtual—so vital to the United States that their incapacitation or destruction would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters. Key resources are publicly or privately controlled resources essential to minimal operation of the economy and the government.[3]

CIKR is organized into 17 sectors that together provide essential functions and services supporting various aspects of the U.S. Government, economy, and society. (See Table A-1 for a full list of sectors and designated Sector-Specific Agencies (SSAs).)

Processes outlined herein apply to Federal departments and agencies during incidents with potential or actual CIKR impacts—and may apply to, or involve, incident managers and security partners[4] at other levels of government and the private sector, including CIKR owners and operators.

CIKR-related processes described in this annex utilize the unified risk-based approach for "steady-state" protection detailed in the *National Infrastructure Protection Plan (NIPP)*. CIKR requirements generated by the threat or incident at hand are coordinated through *NRF* and *NIMS* organizational structures. This applies to activities in the local incident area, as well as response and recovery activities outside the incident area, regionally, or nationally.

Policies

Policies for CIKR protection and preparedness are established through the following authorities: Homeland Security Act of 2002; Homeland Security Presidential Directive (HSPD) 7, "Critical Infrastructure Identification, Prioritization, and Protection"; the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets; the National Strategy for Securing Cyberspace; and other relevant statutes, Executive orders, and Presidential directives.

HSPD-7 charges the Secretary of Homeland Security with responsibility for coordinating the overall national effort to enhance the protection of the CIKR of the United States. The directive also designates SSAs with responsibility for coordinating planning-, preparedness-, and protection-related activities within each of the 17 CIKR sectors. This approach provides the structure needed to address the unique characteristics and operating models of each of the sectors.

---

[2] *National Infrastructure Protection Plan (NIPP)*, 2006, Glossary, pg. 104, defines the term *protection* as "actions to mitigate the overall risk to CIKR assets, systems, networks, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the *NIPP*, protection includes actions to deter the threat, mitigate vulnerabilities, or minimize consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety, and implementing cyber security measures, among various others."

[3] *NIPP*, 2006, Glossary of Key Terms, is the source for the definitions of critical infrastructure and key resources. These definitions are derived from the provisions of the Homeland Security Act of 2002 and HSPD-7.

[4] As defined in the *NIPP*, security partners include Federal, State, regional, tribal, local, or international government organizations; private-sector owners and operators and representative organizations; academic and professional entities; and not-for-profit and private volunteer organizations. Regional security partnerships include a variety of public-private sector initiatives that cross jurisdictional and/or sector boundaries.

Further information on a variety of statutes, strategies, and directives that are applicable to CIKR protection and restoration are included in Appendix 2A of the *NIPP*.

This annex does not alter or supersede existing:

- Statutory responsibilities for CIKR protection, incident management, emergency management, or other related functions under the law.
- Regulatory, contractual, or other legal relationships between Federal agencies and the private sector.
- International agreements, treaties, or other agreements for incident management or between the U.S. Government and other countries.

The following sections provide an overview of the general authorities that guide CIKR-related activities in the context of the *NRF.* This includes the *NIPP*, developed as the implementing structure for steady-state CIKR protection; the Robert T. Stafford Disaster Relief and Emergency Assistance Act; and the Defense Production Act.

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.

In fact, 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 enable 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 risk management framework used to implement *NIPP* steady-state CIKR protection efforts and provide the CIKR protection and restoration dimension for incident management activities under the *NRF*.
- The sector partnership model that encourages the use of Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), and cross-sector coordinating councils to create an integrated national framework for CIKR preparedness, protection, and restoration across sectors.
- The networked approached to CIKR information sharing that provides for multidirectional CIKR-related exchanges of actionable intelligence, alerts, warnings, and other information between and among various *NIPP* partners including: SSAs; State, tribal, and local entities; the Intelligence Community; law enforcement; Emergency Support Functions (ESFs); other Federal agencies and departments; and CIKR owners, operators, and sector-based information-sharing mechanisms.[5]

[5] CIKR sectors rely on information-sharing mechanisms such as Information Sharing and Analysis Centers (ISACs), which provide operational and tactical capabilities for information sharing and, in some cases, support for incident response activities. Originally recommended by Presidential Decision Directive 63 in 1998, ISACs are sector-specific entities that advance physical and cyber CIKR protection efforts by establishing and maintaining frameworks for operational interaction between and among members and external security partners.

Complementing the *NIPP*, supporting SSPs provide the specific mechanisms required for full implementation of the *NIPP* risk management framework within each CIKR sector and are developed by designated SSAs in close collaboration with sector security partners, ESFs, and other Federal agencies and departments.

The Value Proposition

Prevention, response, restoration, and recovery efforts are most efficient and effective when there is full participation of government and industry partners. The "value proposition" set forth in the *NIPP* articulates the mutual benefits to government and private sector for engaging in preparedness and response activities. In accordance with these principles, the Federal Government:

- Provides owners and operators timely, accurate, and actionable all-hazards information.
- Ensures owners and operators are engaged at senior executive and operational levels primarily through their respective SCCs and GCCs.
- Articulates benefits of a risk-based, cross-sector approach to preparedness, resilience, and protection.
- Works with owners and operators to clearly establish priorities for prevention, protection, and recovery.
- Provides specialized technical expertise for CIKR-related preparedness, protection, and recovery.
- Coordinates with international allies and owners and operators on CIKR priorities, risk assessments, mitigation, and restoration and recovery activities.

General Process for Requesting Federal Assistance

CIKR-related preparedness, 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 Federal, State,[6] tribal, or local authorities in certain specific circumstances.

Robert T. Stafford Disaster Relief and Emergency Assistance Act.[7] Disaster assistance programs generally offer support for incident-related repair, replacement, or emergency protective services needed for infrastructure owned and operated by government entities.

Stafford Act principles permit consideration of private-sector requests for assistance, but the application of these legal principles does not guarantee that needs or requests from private-sector entities will be met in all cases. A private-sector CIKR owner or operator may receive direct or indirect assistance from Federal Government sources when the need:

- Exceeds capabilities of the private sector and relevant State, tribal, and local governments;
- Relates to immediate threat to life and property;

[6] Consistent with the definition of "State" in the Homeland Security Act of 2002, all references to States within the CIKR Support Annex are applicable to territories and include by reference any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the U.S. Virgin Islands, Guam, American Samoa, the Commonwealth of the Northern Mariana Islands, and any possession of the United States (Homeland Security Act of 2002).

[7] Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended by Public Law 106-390,April 2007; § 5170b. ESSENTIAL ASSISTANCE (Sec. 403).

- Is critical to disaster response or community safety; and
- Relates to essential Federal recovery measures.

The process for coordinating requests for assistance and information from private-sector CIKR owners and operators is described in the Concept of Operations section of this annex.

The Defense Production Act (DPA) provides specific authority to expedite supply and strengthen production capabilities for CIKR protection and restoration activities.[8] These authorities include use of the following:

- Priority ratings in the Defense Priorities and Allocations System on contracts and orders for industrial resources.[9]
- Financial incentives to expedite deliveries and expand supplies of materials and services.
- Agreements by the private sector to share information to coordinate management of critical supplies.
- Private-sector experts in government emergency preparedness, response, and recovery activities.

The Department of Homeland Security (DHS)/Federal Emergency Management Agency coordinates DPA authorities related to incident management before and during an incident, including: providing priority ratings on contracts and orders for industrial resources in cooperation with the Department of Commerce or relevant SSAs; developing guidance and procedures; coordinating DPA plans and programs; and providing technical assistance for all appropriate Federal agencies under the *NRF* and *NIPP*.

CONCEPT OF OPERATIONS

The concept of operations describes specific organizational approaches, processes, coordinating structures, and incident-related actions required for the protection and restoration of CIKR assets, systems, networks, or functions within the impacted area and outside the impacted area at the local, regional, and national levels. The processes described herein are detailed further in standard operating procedures, field guides, and other related guidance developed collaboratively by DHS and the cooperating agencies to this annex.

The concept of operations uses the organizational structures and information-sharing mechanisms that are established in the *NIPP* for identifying, prioritizing, protecting, and restoring the Nation's CIKR and describes protocols to integrate these steady-state organizational elements with *NRF* incident management organizational structures and activities.

Specifically, the concept of operations focuses on processes and actions for CIKR-related:

- Situational awareness.

[8] The Defense Production Act of 1950 (codified as amended by the Defense Production Act Reauthorization of 2003) is the primary authority to ensure the timely availability of resources for national defense and civil emergency preparedness and response. The DPA defines "national defense" to include critical infrastructure protection and restoration, as well as activities authorized by the emergency preparedness sections of the Stafford Act. Consequently, DPA authorities are available for activities and measures undertaken in preparation for, during, or following a natural disaster or accidental or man-caused event.

[9] The Defense Priorities and Allocations System regulation found in 15 CFR Part 700 implements the priorities and allocations authority of the DPA, ensures the timely availability of industrial resources for approved programs, and provides an operating system to support rapid industrial response to a national emergency.

- Impact assessments and analysis.
- Information sharing.
- Requests for assistance or information from private-sector CIKR owners and operators.

General

Addressing CIKR-related prevention, protection, preparedness, response, and recovery requires cooperation and collaboration between and among CIKR entities. A primary objective of this collaborative effort between the private-sector owners and operators; State, tribal, and local governments; nongovernmental organizations; and the Federal Government is to ensure that resources are applied where they offer the most benefit for mitigating risk, deterring threats, and minimizing the consequences of incidents.

DHS is responsible for leading, integrating, and coordinating the overall national effort to enhance CIKR protection, including developing and implementing comprehensive, multitiered risk management programs and methodologies; developing cross-sector and cross-jurisdictional protection guidance and protocols; and recommending risk management and performance criteria and metrics within and across sectors. The DHS responsibilities for CIKR support that are most applicable during incident response include:

- Identifying, prioritizing, and coordinating Federal action in support of the protection of nationally critical assets, systems, and networks, with a particular focus on CIKR that could be exploited to cause catastrophic health effects or mass casualties comparable to those produced by a weapon of mass destruction.
- Establishing and maintaining a comprehensive, multitiered, dynamic information-sharing network designed to provide timely and actionable threat information, assessments, and warnings to public- and private-sector security partners. This responsibility includes protecting sensitive information voluntarily provided by the private sector and facilitating the development of sector-specific and cross-sector information-sharing and analysis systems, mechanisms, and processes.
- Coordinating, facilitating, and supporting comprehensive risk assessment programs for high-risk CIKR, identifying protection priorities across sectors and jurisdictions, and integrating CIKR protective programs with the all-hazards approach to domestic incident management described in HSPD-5.
- Identifying and implementing plans and processes for threat-based increases in protective measures that align to all-hazards warnings, specific threat vectors as appropriate, and each level of the Homeland Security Advisory System (HSAS).
- Conducting modeling and simulations to analyze sector, cross-sector, and regional dependencies and interdependencies, to include cyber-related issues, and sharing the results with security partners, as appropriate.
- Integrating national efforts for the protection and recovery of CIKR, including analysis, warning, information sharing, vulnerability reduction, and mitigation activities and programs.
- Documenting and sharing lessons learned from exercises, actual incidents, and predisaster mitigation efforts and applying those lessons, where applicable, to CIKR protection efforts.

- Working with the Department of State, SSAs, and other security partners to ensure that U.S. CIKR protection efforts are fully coordinated with international partners.

Federal departments and agencies provide support consistent with their CIKR-related statutory or regulatory responsibilities or with their designated functions as SSAs, ESF primary or supporting agencies, or coordinating or cooperating agencies for other related *NRF* Support or Incident Annexes.[10]

SSAs focus on overarching CIKR protection, risk management, and information sharing by working collaboratively with SCCs, GCCs, relevant Federal departments and agencies, State, local, and tribal governments, ESFs, CIKR owners and operators, sector-based information-sharing mechanisms, and other private-sector entities.

SSAs coordinate CIKR efforts within their sectors to deter threats, mitigate vulnerabilities, and minimize consequences of manmade and natural incidents. SSPs specify each sector's approach to the risk management and information-sharing components of incident management.

In cooperation with the DHS Office of Infrastructure Protection (OIP), SSAs collaborate with private-sector security partners to encourage:

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

In the context of incident management, SSAs coordinate with their counterparts designated within various *NRF* and ESF, Incident, or other Support Annex functions, as appropriate.

ESFs are activated to provide support for evolving CIKR-related incident management requirements by:

- Providing authorities, resources, program implementation, and support required for infrastructure-related response, recovery, and restoration within the impacted area.
- Serving as key points of coordination to address CIKR issues and concerns relating to the impacted area.
- Coordinating and collaborating with DHS; SSAs; owners and operators; State, tribal, and local entities; ESFs; and others as required to address CIKR concerns that fall within the scope of their ESF or other *National Response Framework*-related responsibilities.

State, tribal, and local government entities establish security partnerships, facilitate information sharing, and enable planning and preparedness for CIKR protection within their jurisdictions. State governments are responsible for:

- Developing and implementing statewide or regional CIKR protection programs integrated into homeland security and incident management programs.

[10] Further discussion of specific Federal department and agency support for the CIKR support activities is in the Roles and Responsibilities section of this annex.

- Serving as crucial coordination hubs, bringing together prevention, preparedness, protection, response, and recovery authorities, capacities, and resources among local jurisdictions, across sectors, and across regional entities.

- Acting as conduits for requests for Federal assistance when the threat or incident situation exceeds the capabilities of public- and private-sector security partners in their jurisdictions.

- Coordinating with the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) to ensure full integration with national- and regional-level CIKR prevention, protection, response, and restoration efforts.

Tribal governments are responsible for public health, welfare, safety, CIKR protection, and continuity of essential services within their jurisdictions.

Local governments usually are responsible for emergency services and first-level responses to CIKR incidents. In some sectors, local governments own and operate CIKR such as water, wastewater, and storm water systems and electric utilities, and are responsible for initial prevention, response, recovery, and emergency services provision.

Private-sector CIKR owners and operators are responsible at the corporate and individual facility levels for risk and incident management planning, security, and preparedness investments. Other activities that form part of business and continuity of operations planning activities include:

- Developing and revising business continuity and emergency management plans to address direct effects of incidents and critical dependencies and interdependencies at sector, enterprise, and facility levels.

- Building increased resiliency, backup capabilities, and redundancy into business processes and systems.

- Maintaining coordination with incident management, information-sharing, and CIKR protection programs.

- Reporting CIKR status using established mechanisms for inclusion in the national common operating picture (COP).

- Developing and coordinating CIKR protective and emergency-response actions, plans, and programs.

- Guarding against insider threats.

- Providing technical expertise to DHS, SSAs, ESFs, and other Federal, State, tribal, and local entities.

- Identifying CIKR and prioritizing related protection and restoration activities.

ORGANIZATION

National Level

National organizational structures described in the *NRF* and *NIPP* provide formal and informal mechanisms for public- and private-sector coordination, situational awareness, impact assessments, and information sharing in regard to CIKR-related concerns on a sector-by-sector and/or a cross-sector basis.

This coordination allows for broader engagement in one or more affected sectors. It also allows sectors to plan for and quickly react to far-reaching effects from an incident (or multiple incidents) and to alert individual owners and operators of the need to take specific actions to minimize impacts.

CIKR support at the national level involves active participation and coordination across a variety of activities to include the exchange of liaisons, implementation of reporting and information-sharing protocols, and/or physical representation, as required, at the following:

- **National Operations Center (NOC).** Representatives are assigned to various components of the NOC to provide CIKR subject-matter expertise and facilitate coordination, risk assessment, protective measure implementation, and information sharing. These representatives work with SSAs and ESF counterparts to ensure that coordinated CIKR-related communications, planning, and responses occur. (The *NRF* core document provides further discussion of NOC components and functions.)

- **National Response Coordination Center (NRCC).** DHS/OIP assigns a liaison to the NRCC to provide CIKR protection and incident management subject-matter expertise and direct connectivity to the National Infrastructure Coordinating Center, DHS/OIP risk assessment entities, SSA and ESF primary and supporting agencies, and Infrastructure Liaisons deployed to support Joint Field Office functions.

- **National Infrastructure Coordinating Center (NICC).** The NICC is a 24/7 watch coordination center providing integrated CIKR-related situational awareness and national-level coordination for SCCs, SSAs, owners and operators, and relevant regulatory authorities. The NICC collects sector and cross-sector status information and produces consolidated CIKR reports for incorporation into the Federal interagency COP that is produced by the NOC. During incident response, the NICC works closely with the NRCC to enable overall Federal CIKR response coordination and emergency management program implementation.

- **Department of Justice (DOJ)/Federal Bureau of Investigation (FBI) Strategic Information and Operations Center (SIOC).** DHS/OIP designates representatives, as required, to serve as liaisons to the DOJ/FBI SIOC, which is the focal point and operational control center for all Federal intelligence, law enforcement, and investigative law enforcement activities related to domestic terrorist incidents or credible threats, including leading attribution investigations. The CIKR representatives provide situational awareness, assessment, information-sharing support, and reach-back relating to CIKR status, risk, consequences, and national-level sector and cross-sector priorities.

- **National Coordinating Center for Telecommunications (NCC).** The NCC is a joint government-industry sector forum that provides a mechanism for jointly responding to National Security and Emergency Preparedness (NS/EP) and other communications incidents. The NCC is the operational component of the National Communications System (NCS) and the lead Federal office for communications incident management. (Further details on the NCC and NCS are included in the ESF #2 – Communications Annex.)

- **United States Computer Emergency Readiness Team (US-CERT).** US-CERT is a 24/7 single point of contact for cyberspace analysis, warning, information sharing, incident response, and recovery for security partners. The partnership between DHS and public and private sectors is designed to enable protection of cyber infrastructure and to coordinate the prevention of and response to cyber attacks across the Nation. (Further information on US-CERT incident-related activities is included in the Cyber Incident Annex.)

- **Other Federal Department and Agency Emergency Operations Centers (EOCs).** DHS/OIP designates liaisons, as required, to various Federal EOCs depending on the nature of the threat or incident.

The CIKR support actions described in this annex are applicable to incident management activities required for natural disasters, industrial accidents, and the full spectrum of terrorist events. The CIKR support activities are flexible and adaptable to align to the specific requirements of the incident and function in conjunction with processes as described in the *NRF* and the various Incident Annexes: Biological, Catastrophic, Cyber, Food and Agriculture, Mass Evacuation, Nuclear/Radiological, and Terrorism Incident Law Enforcement and Investigation.

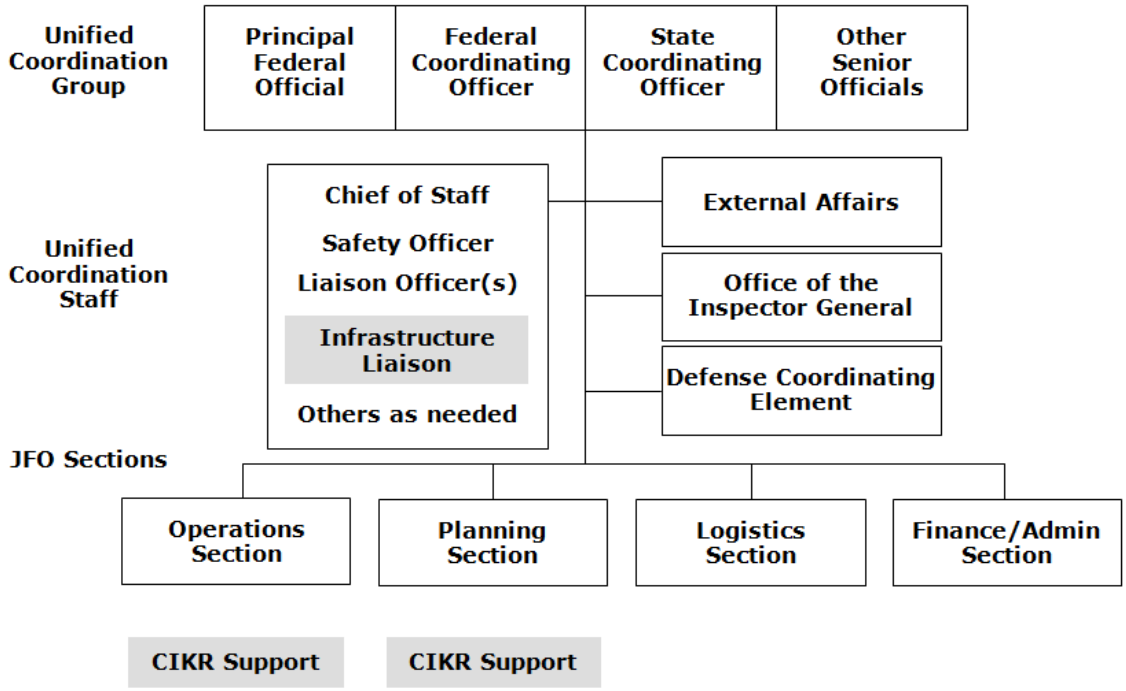
Field Level

The Joint Field Office (JFO), when established, provides the focal point for field-level incident-related CIKR identification, assessment, prioritization, protection, and restoration activities.

CIKR support is also provided, as required, to other incident facilities that are established to support prevention, preparedness, response, and recovery activities. These facilities include, but are not limited to: State, tribal, local, or county EOCs; Incident Command Posts; Area and Unified Commands; and interim operating facilities.

The following section describes the integration of the Infrastructure Liaison functions to support the various JFO sections or field facilities, as well as day-to-day risk management expertise provided by DHS/OIP. (See Figure 1.)

Figure 1. JFO Organization



The Infrastructure Liaison is designated by DHS/OIP and advises the Principal Federal Official (PFO) (if appointed) and the Unified Coordination Group with regard to national- and regional-level and cross-sector CIKR incident-related issues.

The Infrastructure Liaison function is task organized and task dependent on the needs of the incident and the requirements of the PFO, the Unified Coordination Group, and the Incident Management Team.

The Infrastructure Liaison, in collaboration with SSAs and all activated ESFs, provides prioritized recommendations regarding CIKR concerns to the Unified Coordination Group and the PFO (if appointed). The prioritized CIKR recommendations are developed using a collaborative process involving the cooperating agencies to this annex as well as CIKR owners and operators; State, tribal, and local entities; and others as appropriate. The prioritized recommendations are used by the Unified Coordination Group to support incident-related decisionmaking processes and the efficient application of limited resources within the affected area.

The Infrastructure Liaison provides knowledge and expertise regarding unique CIKR considerations, including:

- Impacts to nationally and regionally critical CIKR within the incident area.
- Cross-sector impacts within the incident area.
- Cascading effects that can result in consequences beyond the immediate incident area.
- Interdependencies that require actions beyond those needed for infrastructure restoration within the incident area.

- Potential gaps or overlapping responsibilities among Federal departments and agencies that may function as SSAs, ESF primary or supporting agencies, or statutory or regulatory authorities.[11]

Infrastructure Liaison responsibilities include the following:

- Advising the Unified Coordination Group and the PFO, if appointed, on CIKR issues with national or regional implications or that involve multiple CIKR sectors.
- Acting as the coordination point for CIKR sectors, including private-sector owners and operators that are not otherwise represented in the JFO.
- Serving as the senior advocate in the Unified Coordination Staff for CIKR issues not otherwise raised through the Unified Coordination Group.
- Advising the Unified Coordination Group regarding the prioritization of CIKR protection and restoration issues.
- Providing additional coordination and liaison capabilities to the CIKR sectors for the Unified Coordination Group in addition to the coordination and liaison functions provided by the various ESFs.
- Working with the JFO Section Chiefs and Branch Directors to coordinate between and among CIKR sectors and ESFs.
- Ensuring that information obtained from the NICC and CIKR sectors is integrated into the overall COP for the incident.
- Ensuring sensitive CIKR-related information is handled and safeguarded in accordance with the Protected Critical Infrastructure Information (PCII)[12] Program, Chemical-terrorism Vulnerability Information (CVI),[13] or other appropriate guidelines.

The Infrastructure Liaison assigns personnel as requested by the Unified Coordination Group to facilitate cross-sector and sector-related coordination and integration among ESFs, SSAs, appropriate Federal agencies and departments, and other entities with CIKR-related responsibilities.

[11] See Responsibilities section for discussion of SSA and ESF functions and a matrix of Federal department and agency functions.

[12] The PCII Program, which operates under the authority of the Critical Infrastructure Information (CII) Act of 2002, provides a means for sharing private-sector information with the government while providing assurances that the information will be exempt from public disclosure and will be properly safeguarded. This program defines the requirements for submitting critical infrastructure information as well as the requirements that government entities must meet for accessing and safeguarding PCII.

[13] DHS identifies information that constitutes Chemical-terrorism Vulnerability Information (CVI) to include the following documents when submitted as part of the 6 CFR 27 regulatory compliance process: Security Vulnerability Assessments (SVAs); Site Security Plans (SSPs); documents relating to the Department's review and approval of SVAs and SSPs, including Letters of Authorization, Letters of Approval, and responses to them; written notices; and other documents developed to comply with the interim final regulations; Alternative Security Programs; documents related to inspections and audits; records required to be created and maintained by regulated facilities; sensitive portions of orders, notices, or letters; information developed pursuant to the Top-Screen process; and other information designated as CVI by the Secretary.

DHS/OIP, in coordination with SSAs, provides training and designates Infrastructure Liaisons and other CIKR support from a group that includes DHS/OIP Headquarters and/or field-level staff such as DHS/OIP Protective Security Advisors (PSAs)[14] and individuals with CIKR expertise from other Federal departments and agencies, including SSAs and ESFs, as appropriate.

Infrastructure Liaison functions are task oriented depending on the scope, magnitude, and complexity of the CIKR-related requirements. These functions include, but are not limited to:

- Assisting with onsite assessments of the status of potentially affected or impacted CIKR.
- Deploying to other locations, such as State or local EOCs or the JFO, to provide CIKR subject-matter expertise.
- Providing assessments of local CIKR status to the JFO based on direct observation and coordination with ESFs and CIKR owners and operators.
- Providing CIKR-protection expertise in support of ESF #13 – Public Safety and Security efforts within an impacted area.
- Coordinating with SSAs, ESFs, and appropriate Federal agencies and departments on damage and security assessments to promote communication of assessment results and minimize duplication of effort.

CIKR Support for Incident Management Actions

The CIKR support function is structured to apply the *NIPP* risk management framework to produce prioritized recommendations for CIKR protection and restoration in the context of incident management. DHS, cooperating agencies, and other government and private-sector security partners continuously conduct situational awareness, assessments, analyses, and information-sharing activities and facilitate requests for information and assistance through steady-state activities to better prepare for response, recovery, and restoration actions during an incident.

Key elements of these "steady-state" CIKR support missions include:

Situational Awareness

- Monitoring information flow and threats to become aware of an incident or potential incident.
- Reviewing CIKR data and data inventories.
- Identifying opportunities for mitigation.
- Identifying appropriate response posture for CIKR elements and resources.

[14] PSAs are DHS locally based critical infrastructure and vulnerability assessment specialists assigned to local communities throughout the country. PSAs serve as CIKR liaisons between Federal agencies; State, tribal, and local governments; and the private sector. They contribute to *NIPP*- and *NRF*-related requirements by identifying, assessing, and monitoring CIKR and coordinating protective activities within their respective geographic areas during steady-state operations as well as during incidents.

Assessments and Analyses

- Leveraging institutional knowledge and sector-partner relationships to collect data and assess CIKR needs and vulnerabilities.
- Collaborating in preparation for more indepth assessments and analyses during an incident.
- Reviewing plans to assess projected impacts on CIKR within a potential incident area.
- Developing projected consequences locally, regionally, and nationally by applying the *NIPP* risk management framework to the National Planning Scenarios.

The National Infrastructure Simulation and Analysis Center (NISAC) provides advanced modeling and simulation capabilities for the analysis of CIKR vulnerabilities and interdependencies and the cascading effects of infrastructure loss, damage, or destruction over time based on the National Planning Scenarios.

Information Sharing

- Participating in multidirectional information flow between government and private-sector security partners.
- Developing and providing a comprehensive COP of threats and hazards to CIKR.
- Providing security partners with a robust communications network, including a common set of communications, coordination, and information-sharing capabilities.
- Providing a means for State, tribal, local, and private-sector security partners to be integrated, as appropriate, into the intelligence cycle.

Requests for Information/Assistance

- Facilitating real-time transmission of requests and status.
- Maintaining a comprehensive log and retrievable database of all requests.

During daily operations (non-incident related), the NICC disseminates a range of all-hazards products and CIKR protection information to security partners. Information dissemination includes the following:

- Threat-related and other all-hazards information products to government and private-sector CIKR security partners, as appropriate.
- Reports from the private sector on suspicious activity or potential threats to the Nation's CIKR.
- Requests for information and requests for assistance.

Preresponse/Initial Actions

Transition from steady-state to preresponse incident-related activities begins with warning of a potential incident or the notification of an incident.

CIKR Information, Assessment, and Analytical Products

Examples of DHS information, assessment, and analytical products include:

- **Incident Reports:** Evaluate information received initially through news media, Internet, CIKR owners and operators, and other sources.
- **Spot Reports:** Provide current situation status and operational snapshot assessment of operational CIKR effects from emerging incidents.
- **Threat Warnings:** Fuse all source information to provide analysis of emergent threats on a timely basis.
- **Terrorist Target Selection Matrix:** Identifies sectors prone to different terrorist attack modalities.
- **Attack-Specific Threat Scenarios:** Provide planning and exercise phases for possible attacks with inputs from corporate- or facility-level security officers.
- **Sector-Specific Threat Assessment:** Provides specific and general terrorist threat information for each sector, as well as relevant background information, such as terrorist objectives and motives as they apply to that sector.

Notification and Reporting

DHS, in coordination with the SSAs, is responsible for coordinating CIKR incident notification and information sharing among Federal agencies; State, tribal, and local entities; and CIKR owners and operators. DHS uses established systems, such as the Homeland Security Information Network (HSIN), COP, Critical Infrastructure Warning Network, and other sector-based information-sharing mechanisms, to create CIKR situational awareness in support of incident operations.

Upon notification from the NOC of a potential or actual incident, the NICC coordinates with the SSAs, CIKR sectors (GCCs and SCCs), ESFs, industry partners, and other established information-sharing mechanisms to communicate pertinent information.

Based on the nature and scope of the potential or actual incident, DHS/OIP alerts and, if required, deploys Infrastructure Liaisons or additional CIKR support to various NOC elements, the DOJ/FBI SIOC, other Federal EOCs, or field facilities to ensure full integration of CIKR considerations and to provide situational awareness, assessments, information sharing, and prioritized recommendations.

In support of NOC reporting requirements, the NICC serves as the overall Federal focal point for CIKR incident and status reporting from SSAs, ESFs, CIKR owners and operators, and other appropriate Federal and/or State departments and agencies. The NICC coordinates these inputs with the NRCC and JFO. The following actions occur when reporting starts:

- The NICC alerts SSAs that the reporting process has begun via the Infrastructure Protection Executive Notification Service.
- SSAs coordinate with SCCs, GCCs, ESFs, and established information-sharing and analysis mechanisms in their sector to initiate status reporting and impact assessments. (These can include various sector-identified information-sharing mechanisms such as Information Sharing and Analysis Centers (ISACs) or Information Sharing and Analysis Organizations

(ISAOs).)

- The NICC verifies reported information and compiles the CIKR Situation Report, which is included in the NOC COP and posted to the HSIN.

- Cooperating agencies are responsible for notifying DHS when they receive threat- or incident-related information from within their sectors. The NICC documents these reports, compiles additional details surrounding the suspicious activity or potential threat, and disseminates reports to the CIKR sectors, the NOC, the NRCC, the DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), and DOJ/FBI.

CIKR-related threat analysis is a collaborative function between the DHS Office of Intelligence and Analysis (OI&A) and OIP through the DHS HITRAC, which conducts integrated terrorism threat and risk analysis for all CIKR sectors.

DHS/OI&A works with the intelligence and law enforcement communities to assess national security threats.[15] HITRAC brings together both intelligence and infrastructure specialists to provide an understanding of CIKR sector- and national-level risk. This collaborative function is carried out with:

- Input from private-sector liaison personnel, and on-call subject-matter experts who provide industry-specific expertise.

- Input from the intelligence and law enforcement communities.

- Coordination with existing entities such as NCC, US-CERT, GCCs, SCCs, SSAs, ESFs, and/or other sector-identified information-sharing and analysis organizations such as ISACs.

On the basis of HITRAC analysis, DHS produces information that supports the response to emergent threats or immediate incidents, as well as strategic planning activities focused on enhancing the protection of CIKR over the long term.

CIKR risk assessment and analysis is a collaborative effort between DHS, cooperating agencies to this annex, and other security partners to perform the following:

- Examine existing plans and infrastructure characteristics to assess projected or actual impacts on CIKR in potential incident areas or on CIKR that have been designated as high risk.

- Determine critical failure points within or across CIKR sectors, regional or national cascading effects, and other significant issues that could affect CIKR assets inside and outside the immediate incident area.

The risk assessment and analysis process uses empirical data collection, database development and assessment, modeling, and simulation to inform decisionmaking.

These assessments and analyses support CIKR protection and mitigation actions prior to an incident and timely response actions during an incident. Results of assessments and analyses are provided to the NICC, SSAs, ESFs, emergency managers, CIKR owners and operators, and appropriate Federal and State departments and agencies.

[15] See the Terrorism Incident Law Enforcement and Investigation Annex in the *NRF* for a complete discussion on threat investigation-related actions.

DHS assessments, excluding PCII information, are shared across the sectors through electronic dissemination, posting to HSIN portals, and direct outreach by DHS/OIP sector specialists and DHS/HITRAC analysts. These efforts provide the private sector with timely, actionable information to enhance situational awareness and enable security planning activities

The *NIPP* details protective programs and initiatives that provide the basis for CIKR risk assessment activities during incident management. The following are representative of these key processes:[16]

- **National Asset Database (NADB):** Comprehensive catalog of the Nation's assets, systems, and networks and the primary Federal repository for CIKR information.
- **Buffer Zone Protection Program:** Grant program to provide resources to State, tribal, and local law enforcement and other security professionals to enhance security of priority CIKR facilities.
- **Site Assistance Visits:** Facility-level security assessments to facilitate vulnerability identification and mitigation discussions.

The NISAC provides advanced modeling and simulation capabilities for the analysis of CIKR vulnerabilities and interdependencies and the cascading effects of infrastructure loss, damage, or destruction over time.

During emerging or actual incidents, the NISAC produces assessments that:

- Integrate current situation data with preestablished infrastructure modeling, simulation, and analysis.
- Project consequences of an incident, preincident or postincident.
- Inform response and recovery activities after an incident has occurred.

Additional CIKR support preresponse actions include:

- Testing and exercising information-sharing and communication processes and systems with CIKR protection security partners.
- Developing and testing continuity of business plans, including identification and preparation of alternate sites and backup locations, as appropriate.
- Recommending and implementing elevated protective measures to align the CIKR protective posture with all-hazards warnings, specific threat indications, and different levels of the HSAS.
- Preparing the Infrastructure Liaison and CIKR support to deploy to the JFO.

RESPONSE ACTIONS

CIKR situational awareness and reporting are essential to providing a consolidated COP during an incident. The NICC provides coordinated CIKR status and infrastructure-related information supporting the COP by serving as the national collection, reporting, and distribution point for CIKR-related information.

[16] See Appendix 3B in the *NIPP* for a complete listing and description of each.

The NICC provides a focus on CIKR-related impacts both within the incident area and across the Nation as a whole. It provides mechanisms to integrate and cross-reference CIKR-related information from various official sources to minimize duplicative reporting and information collection.

In support of incident response, the NICC performs the following:

- Hosts a daily teleconference to provide owners and operators and SSAs, ESFs, other Federal departments and agencies, and State, local, and tribal governments with a collated CIKR status and facilitates cross-sector discussions.
- Provides tailored situation assessments for the CIKR section of the DHS Situation Report.
- Facilitates assessment sessions between SSAs; State, local, and tribal governmental entities; and DHS Sector Specialists.
- Reconciles CIKR information and reporting with the NRCC.
- Consolidates SSA reports for integration into overall national-level reporting, including the COP.
- Provides security partners with Web-enabled access to a variety of incident-related information.

SSAs, ESFs, and other Federal departments and agencies maintain situational awareness of their area of responsibility and factor information from official field-level sources into their overall sector-level reporting.

Established protocols for SSA CIKR reporting include producing field-level reports (as applicable) and analyzing the national-, regional-, and sector-level CIKR implications. All information is coordinated with appropriate entities. These products are created for, but not limited to, the following categories of information:

- Current status/damage assessments
- Restoration activities
- Key issues and concerns

CIKR incident reporting cycles are synchronized with the overarching reporting requirements established by the NOC and NRCC at the national level and by the JFO or multiple JFOs, as required, at the field level.

Field-level reporting on damage assessments and status of restoration efforts within the affected area is generally through the ESF structure, using established reporting protocols at the JFO and the NOC/NRCC. These field-level reports are the basis for CIKR-related damage assessments and response and recovery activities.

CIKR Incident-Related Assessments. When an incident occurs, assessments of sector-specific and cross-sector impacts are coordinated by DHS/OIP in collaboration with SSAs, GCCs, SCCs, ESFs, other appropriate agencies, and security partners. The assessments are supported by the integration of multiple data sets, to inform decisionmakers at all levels as they develop action recommendations.

DHS/OIP uses the *NIPP* risk management framework to analyze the implications that CIKR affected by the incident may have on a regional or national basis. These include assessments to determine:

- Risk (consequence, vulnerability, and threat).
- Interdependencies.[17]
- Cascading or secondary effects on critical systems or infrastructure.
- Impact analyses inside and outside the affected area.

At the national level, the NISAC may conduct updates to existing assessments or perform new assessments to provide the most current situation data to decisionmakers.

NISAC products are made available to the NOC Planning Element, the Unified Coordination Group through the Infrastructure Liaison, and, as appropriate, other incident management and security partners involved in response activities.

Information included in the NADB is used to facilitate CIKR identification within the impacted area and across the Nation that may be directly or indirectly affected by the cascading effects of the incident.

Regional-level assessments during response activities help inform leadership as to the best possible prioritization for CIKR recovery and restoration.

Damage assessments are conducted by various teams that survey and assess impacts to CIKR. The teams include, but are not limited to, the following:

- Joint preliminary damage assessment teams (provide estimate of damages eligible for Federal assistance under the Stafford Act).
- Engineering teams (assess impacts to specific CIKR).
- Building process engineering teams (analyze structural vulnerability and potential mitigation recommendations).
- Environmental impact assessment teams.

The Infrastructure Liaison may provide CIKR expertise and analyses to these teams as required.

The Infrastructure Liaison, in consultation with SSAs, ESF representatives, and others, as well as DHS/OIP representatives positioned within the various NOC components, develops and provides priorities recommendations for CIKR-related actions to the Unified Coordination Group. These recommendations are based on ongoing access to national-level risk assessment and evaluation tools used to provide sector-by-sector and cross-sector evaluations of risk to and effects on CIKR within and outside the incident area. These assessments are used to analyze CIKR protection and restoration needs, support the efficient prioritization of efforts to meet these needs, and monitor the execution of support to CIKR owners and operators.

Requests for assistance from CIKR entities for incident-related requirements can be addressed through direct actions by owners and operators or with government assistance provided by

[17] Interdependency as defined in the *NIPP* is the multi- or bi-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly.

Federal, State, tribal, or local authorities in certain specific circumstances. These requests must be directed to the appropriate Federal, State, tribal, and/or local decisionmakers with authority to consider and adjudicate requirements in the context of competing priorities.

At the State, tribal, or local level, requests for assistance from CIKR owners and operators typically will be acted upon by State or local primacy or regulatory agencies and/or within multiagency coordination centers in the affected area, such as the State or local EOC. CIKR owners and operators of public or quasi-public infrastructure in the affected area are required to follow the established application process for Stafford Act assistance.

At the Federal level, requests may be addressed through existing authorities of Federal departments or agencies or through application of the Stafford Act. The JFO, when activated, is the Federal focal point at the field level for considering, adjudicating, and acting upon requests for assistance. In cases where a JFO has not been established, the NRCC provides the national-level forum for decisions and actions relating to the Federal assistance or resource support.

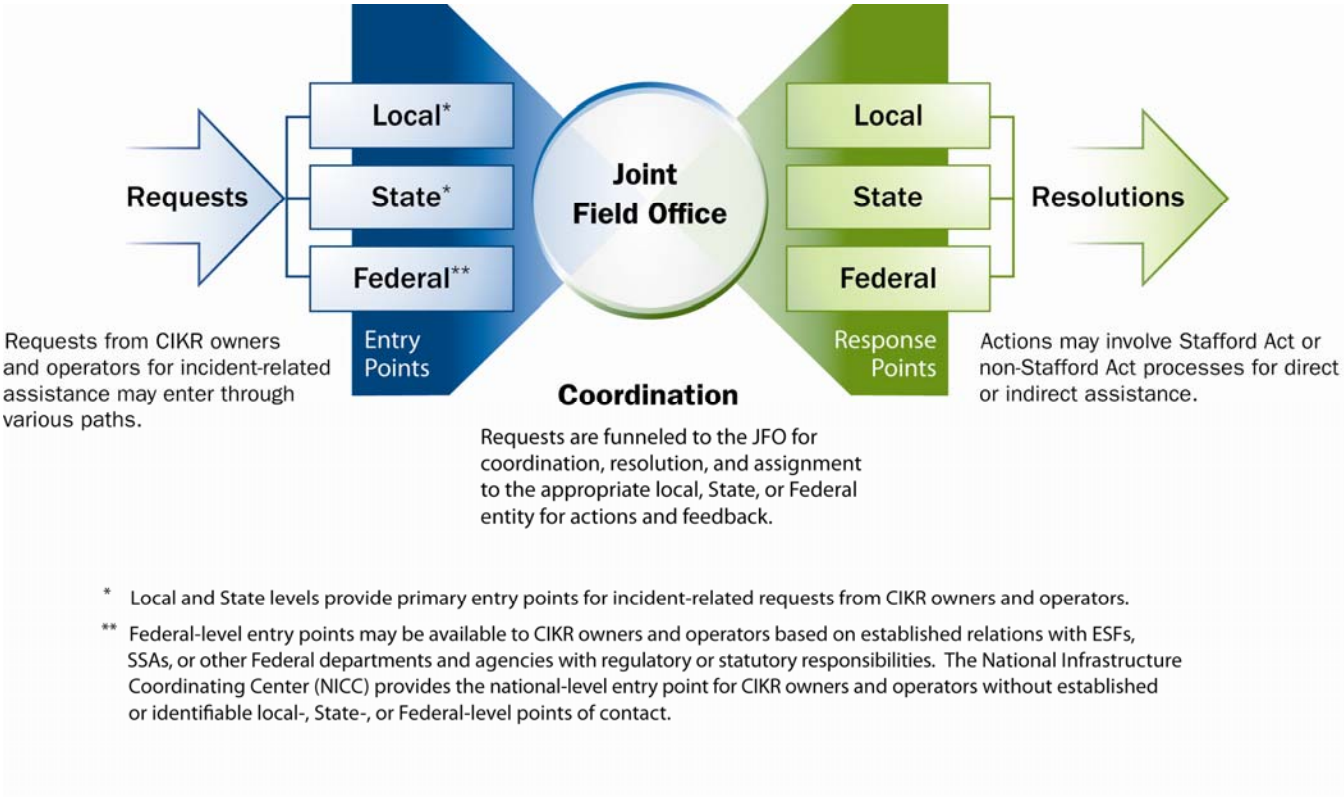
The Federal Coordinating Officer or Federal Resource Coordinator at the JFO (or the Operations Section Chief at the NRCC before establishment of a JFO) determines whether a request submitted by the State on behalf of a CIKR owner or operator or by a Federal department or agency through ESF #5 – Emergency Management is valid and supportable.

When the request involves application of Stafford Act authorities, the determination is based on consideration of a number of factors that include, but are not limited to, the following questions:

- Is assistance essential to public health and safety?
- Is a specific authority, such as the Stafford Act or DPA, needed for the request?
- Does the JFO have the capability to provide resources through Stafford Act authorities or to facilitate non-Stafford Act coordination to meet the requirement?
- Does the request align with current response, recovery, and restoration priorities established by the Unified Coordination Group or through the NRCC if the JFO is not established?
- Is the Federal Government the most appropriate level to provide resources to meet the requirement? If so, what ESF is the most appropriate to coordinate the request?
- What is the reimbursement mechanism for ESF or other Federal department or agency support?
- Which other officials are participating in the Unified Coordination Group or at the national level and are able to commit agency authorities or resources that would be needed to support the request?
- Does the request align with the current incident-management priorities?
- Does the requester have the capability to provide resources on its own?
- Are there alternative means and timing available to provide the requested assistance?
- What are the benefits or costs of providing assistance to a local community's resources, capabilities, and/or economy and meeting critical regional or national CIKR needs?

- What are the benefits or costs to a community or region of redirecting the requested resources or capabilities from other requirements?

Figure 2. Requests for Assistance From CIKR Owners and Operators



CIKR-related requests for incident-related assistance may come in through various paths at the local, State, regional, or national level. (See Figure 2.) Requests for assistance or information from CIKR owners and operators may relate to a variety of incident-related needs such as requirements for security, impact area access, fuel, or accommodations for crews needed to perform critical repair work.

Regardless of the entry point, requests are coordinated, tracked, and channeled to the appropriate authorities and CIKR subject-matter experts from the appropriate cooperating agencies for resolution and determination of the best course of action.

Generally, State, tribal, and local authorities and/or SSAs, ESF primary or supporting agencies, or other Federal Government entities, including those with regulatory responsibilities, provide primary entry points for these requests.

Entry points and processing paths, depicted in Figure 2 above, are as follows:

- Local, State, and tribal officials, in most cases, determine the appropriate level at which to consider and/or coordinate support to ensure the most effective response to requests for assistance from private-sector CIKR owners and operators. Local authorities may elect to fill valid requests using local resources. If local resources are not available, they may utilize mutual aid and assistance agreements to access additional resources.

- If all local resources are depleted, including those that can be acquired through mutual aid and assistance agreements, then local officials may forward the request to the State for action. The State may also elect to fill valid requests using its assets or request support from another State using the Emergency Management Assistance Compact or other preestablished memorandums of understanding. If assistance is not available at the State level, officials may forward the request to the JFO (or Regional Response Coordination Center (RRCC) or NRCC if the JFO is not established) to determine whether the request is eligible for Federal assistance.

- In CIKR sectors where there is no primary State or local point of contact, representatives of the various ESF, SSA, and/or Federal regulatory authorities positioned within the NRCC, RRCCs, and/or the JFO serve as points of contact. In these sectors, owners and operators communicate requests through the established relationship with the Federal department or agency that has primary responsibility for a specific functional area. The SSA and/or ESF may address a CIKR-related request it deems to be valid using its own authorities or resources, if applicable, or may forward the request to the NRCC or the JFO through ESF #5 for further consideration.

The NICC provides an alternate avenue for CIKR owners and operators to communicate needs for assistance, and is the most appropriate path in situations in which CIKR owners and operators do not have either mechanisms for coordination at the local or State levels or established linkages to ESFs, SSAs, or other Federal entities that can help communicate and facilitate the requests. The NICC is the appropriate point of entry in the following circumstances:

- Before JFO establishment.

- National-level, nongeographic-specific incidents that do not require JFO establishment (such as response to a terrorist threat or a biological, agricultural, or other widespread incident).

- Specific CIKR asset, system, network, or function of national significance based on scope or potential impact or criticality to national security or economic vitality.

Requests submitted to the NICC are routed, as appropriate, through the NRCC or the Unified Coordination Group, and the Infrastructure Liaison for coordination with the appropriate ESF, SSA, and other coordinating and cooperating agencies.

The NICC maintains an automated log of all requests for assistance or information it has processed. This log is shared with the Infrastructure Liaison at the JFO and DHS/OIP to maintain ongoing situational awareness, avoid duplication of effort, and enable coordination of actions relevant to the request.

Prior to full activation of the JFO, the NICC works closely with the NRCC to coordinate requests for assistance from CIKR owners and operators.

Activation and Deployment. DHS/OIP, in coordination with the NRCC and the JFO, designates and deploys staff to support Infrastructure Liaison activities at the national and field levels. These deployed field elements maintain close coordination with national elements at the NOC, NRCC, and NICC.

The Infrastructure Liaison(s) support prevention, preparedness, response, and recovery in the following manner:

- Facilitating CIKR situational awareness, assessment, and information sharing by providing liaison with the DOJ/FBI SIOC and other Federal EOCs, initial operating facilities, or other incident management facilities established consistent with the specific threat or incident.

- Facilitating the CIKR information-sharing process through coordination with JFO sections, ESF and sector representatives, CIKR owners and operators, and other security partners at the field level.

- Providing information on CIKR risk, damage, and service disruption within the impact area. This information is coordinated with national elements outside the affected area including identification of CIKR that may pose a higher level of concern as a result of the incident.

- Facilitating development of courses of action relating to CIKR restoration to provide continuity of essential goods and services.

- Providing a point of contact for CIKR sectors that do not have direct alignment with a specific ESF (such as postal and shipping, commercial facilities, and national monuments and icons).

- Participating, as requested, in preliminary damage assessments, rapid needs assessment, Federal Incident Response Support Teams, and others.

- Coordinating with ongoing damage and security assessments to eliminate duplication of effort and promote sharing of assessment results.

- Providing situational awareness in regard to CIKR assets and cross-sector concerns to the JFO, in coordination with the NRCC and DHS/OIP.

- Participating in JFO senior leadership and activities required for the operational planning cycle and development of the Incident Action Plan.

- Monitoring execution of support to CIKR entities as required by the Incident Action Plan.

- Following processes to ensure the proper handling and safeguarding of sensitive CIKR-related information in accordance with PCII, CVI, or other appropriate guidelines.

- Assessing CIKR protection and restoration needs to support efficient prioritization of efforts to meet requirements.

- Directing activities of DHS/OIP field staff in geographic branches (as designated by the JFO) based on priorities established by the Infrastructure Liaison.

- Resolving information discrepancies relating to status of CIKR restoration and protection activities in various sections of the JFO.

- Participating in JFO "hotwashes" to identify CIKR-related issues.[18]

- Maintaining automated linkage to the NICC.

- Tracking and coordinating with ESFs and SSAs on private-sector requests for assistance and requests for information when required to provide cross-sector facilitation.

[18] Interagency meetings called "hotwashes" are convened to identify critical issues, lessons learned, and best practices associated with incident management activities. Hotwashes typically are conducted at major transition points over the course of incident-related operations, and include Federal, State, tribal, local, and other participation as appropriate.

- Coordinating with ESFs, SSAs, and appropriate Federal agencies to identify and aggregate CIKR-related concerns and security requirements.

The Infrastructure Liaison develops CIKR protection and restoration priority recommendations in coordination with JFO Section Chiefs or Branch Directors and representatives of ESF primary and supporting agencies. Infrastructure Liaison coordination activities with ESF representatives include:

- Developing coordinated inputs for the Incident Action Plan.

- Coordinating with activated ESFs on recovery, restoration, and security requirements, specifically to include coordinating with:

  - ESF #1 for transportation infrastructure.
  - ESF #2 on the status of communications infrastructure operations.
  - ESF #3 on infrastructure risk and vulnerability assessments.
  - ESF #8 on status and impacts on the public health and medical community.
  - ESF #10 on CIKR facility or structure decontamination for incidents where they have been contaminated by hazardous materials.
  - ESF #11 on agricultural, natural and cultural resources, and historic properties issues.
  - ESF #12 on impact assessments for the energy infrastructure.
  - ESF #13 on efforts to analyze protection requirements and/or enhance security and protection measures for CIKR within and outside the affected area.
  - ESF #14 on long-term community recovery, including impacts on commercial and banking and finance entities.

(Further discussion of specific ESF responsibilities is included in the respective ESF Annexes to the *NRF*.)

Incident-Related Communication, Including Emergency Public Information. The DHS Office of Public Affairs (PA), at the national level, works in conjunction with DHS/OIP and the DHS Assistant Secretary for the Private Sector to provide timely public information to the CIKR sectors and their security partners (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 outlined in the *NRF* Public Affairs Support Annex to ensure coordination with Federal, State, tribal, and local entities.

DHS/PA communication actions include the following:

- Providing the overarching coordination lead for incident communications to the public 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 and GCCs.

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 ISACs, major trade associations and other private-sector organizations as appropriate, and State, tribal, and local regulatory 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.

POSTRESPONSE ACTIONS

As an incident is brought to closure, incident-related activities transition back from response to steady state. Concurrently, the after-action report is prepared.

Demobilization. CIKR-related liaison, coordination, and information-sharing activities continue in support of JFO functions as required and continue at a level consistent with ongoing efforts.

Infrastructure Liaison actions include the following:

- Participating in JFO "hotwashes" to identify critical CIKR-related issues.
- Evaluating CIKR support staffing requirements and making recommendations for redeployment of staff members to the Unified Coordination Group.
- Preparing plans for deactivation and transfer of responsibilities to DHS/OIP, the NICC, or other elements, as appropriate.
- Coordinating with the JFO Planning Section on CIKR-related long-term recovery efforts.
- Providing input to the local or regional demobilization strategy.
- Informing onsite leadership or a designated representative of the overall DHS/OIP demobilization strategy.

Non-DHS/OIP deployed response elements execute their respective organizational demobilization plans.

The NICC maintains the reporting and information-sharing processes in coordination with the NOC, NRCC, and JFO requirements. As requirements diminish, the NICC notifies cooperating agencies of reporting requirement changes and other incident-related activities throughout the incident closure process.

After-action reports are developed following an incident to detail operational successes, problems, and key issues affecting management of the incident. After-action reports include appropriate feedback from all Federal, State, tribal, local, nongovernmental, and private-sector partners participating in the incident.

Procedures to complete after-action reports include:

- DHS/OIP organizing and managing a template to capture CIKR data.

- CIKR security partners collecting/collating and submitting relevant after-action data[19] throughout the incident life cycle.

- CIKR security partners participating in after-action evaluation sessions at the national and the regional levels.

DHS/OIP coordinates review meetings after the conclusion of the incident and publication of after-action reports to ensure that lessons learned concerning CIKR issues throughout the incident are accurately captured and integrated into plans, assessments, and procedures across all agencies.

The NICC ensures that after-action information is posted to the network and is available to security partners as appropriate.

RESPONSIBILITIES

Coordinating Agency: DHS

DHS, as the department charged with overarching responsibility for coordination of CIKR identification, protection, and prioritization, is the coordinating agency for the CIKR Support Annex. In this context, DHS, in collaboration with SSAs, is responsible for the following:

- Developing plans, processes, guidance, and partnerships and facilitating coordinated CIKR protection with the private sector at the strategic, operational, and tactical levels both during steady-state, day-to-day operations and during incident response.

- Sharing and protecting information on sensitive CIKR-related matters such as threats, warnings, response activities, and operational status—before, during, and after an incident.

- Identifying, training, designating, and deploying personnel to support the Infrastructure Liaison role and staff members in the JFO and its area of operations.

- Informing and educating private-sector owners and operators; State, tribal, and local governments; and other security partners on *NRF* and *NIPP* content, and encouraging and facilitating the development and coordination of equivalent planning for CIKR protection both for steady-state operations and during an incident.

- Coordinating and conducting national and regional incident management exercises, training events, and working meetings with the private sector and State, local, tribal, and select foreign governments.

- Developing methodology to track requests for information from or assistance to CIKR facilities to help ensure that responding departments and agencies are aware of requests from or visits made to CIKR facilities.

- Developing, implementing, and operating information-sharing and communication strategies, processes, and systems with CIKR security partners.

Cooperating Departments, Agencies, and Organizations

This section discusses responsibilities of all cooperating agencies/organizations, including those that are specific to SSAs, ESFs, other departments and agencies, and CIKR owners and

[19] Data relevant for after-action reports can originate from written reports, meeting notes, interviews, briefings, observations, communications, and other recordings.

operators. In addition to the cooperating agencies designated in this section, departments and agencies with primary responsibility for each of the ESFs are responsible for developing and maintaining working relations with associated private-sector counterparts and for exercising ESF mechanisms to enable the recovery of CIKR. Cooperating agencies for this annex may concurrently have responsibilities as ESF primary or supporting agencies, or as coordinating or cooperating agencies for other *NRF* Support or Incident Annexes.

In accordance with the *NRF*, the range of responsibilities for cooperating agencies/organizations includes the following:

- Working in collaboration with CIKR private-sector security partners, owners, and operators.
- Conducting operations relating to CIKR identification, prioritization, and protection using their own or Stafford Act authorities, subject-matter experts, capabilities, or resources.
- Participating in planning for short-term and long-term CIKR-related incident management, response, recovery, and restoration functions and for the development of supporting operational plans, standard operating procedures, checklists, or other job aids.
- Providing available personnel, equipment, or other resource support, as appropriate.
- Participating in training and exercises aimed at continuous improvement of CIKR-related prevention, response, and recovery capabilities.
- Using established Incident Command System, EOC, NOC, and/or JFO information-sharing protocols to notify other agencies that may have overlapping responsibilities for a CIKR asset, system, or network of 1) intended actions concerning requests for information from or assistance to a CIKR facility, or 2) field visits to such facilities.
- Nominating to DHS for review and evaluation new technologies or procedures that have the potential to improve performance within or across CIKR protection functional areas.

Sector-Specific Agencies

In the context of this annex, SSAs are responsible for the following incident-related actions:

- Identifying, prioritizing, and coordinating Federal action in support of the protection of nationally critical assets, systems, and networks, with a particular focus on CIKR that could be exploited to cause catastrophic health effects or mass casualties.
- Collaborating with State and private-sector security partners to facilitate real-time incident notification, as well as CIKR protection expertise and risk assessment methods in the sector.
- Establishing coordination mechanisms for CIKR protection during response and recovery.
- Participating in planning and implementation of recovery measures, as required, in coordination with processes established in the *NRF* for related ESF Annexes and other Incident and Support Annexes.
- Providing comprehensive risk assessment and management programs, as appropriate and consistent with the unique sector landscape, that can be used for identifying protection priorities for incident-related situations.

- Working with all security partners to develop plans and processes for threat-based increases in protective measures that align the CIKR protective posture to all-hazards warnings, specific threat indications, and the different levels of the HSAS.

Emergency Support Functions

In the context of this annex, ESF primary and supporting departments and agencies are responsible for developing and maintaining working relationships with associated State, local, tribal, and private-sector counterparts and exercising their ESF mechanisms to enable the recovery of CIKR. This includes, but is not limited to, the following:

- Establishing and implementing processes to ensure full integration of CIKR-related activities relevant to the specific ESF and including these processes in the respective ESF Annex to the *NRF*.
- Coordinating with CIKR owners and operators, as appropriate.
- Coordinating with the DHS/OIP representative at the NOC and with the JFO Infrastructure Liaison.
- Providing CIKR-related damage assessments and operating status in the affected area using established JFO and NOC reporting procedures.
- Responding to or coordinating CIKR-related requests for assistance as relevant to the specific ESF.

COOPERATING AGENCIES/ORGANIZATIONS

Agency	Functions
Department of Agriculture (USDA)	• Serves as the SSA for the Agriculture and Food Sector. • Advises and assists in assessing impacts to meat, poultry, and egg products.
Department of Commerce	• Works with DHS and private-sector, research, academic, and government organizations to improve cyber system technology and promote other CIKR protection efforts, including use of authority under the DPA to ensure timely availability of industrial products, materials, and services to meet homeland security requirements and address economic security issues. • Supports the Emergency Alert System through the National Oceanic and Atmospheric Administration (NOAA)/National Weather Service and provides public dissemination of critical preevent and postevent information over the all-hazards NOAA Weather Radio system, the NOAA Weather Wire Service, and the Emergency Managers Weather Information Network.
Department of Defense (DOD)	Serves as the SSA for the Defense Industrial Base Sector, when requested, and, upon approval of the Secretary of Defense, provides Defense Support of Civil Authorities (DSCA) during domestic incidents. Accordingly, DOD is considered a cooperating agency under this annex.
Department of Education	• Serves as the Subsector-Specific Agency for education facilities, providing guidance and information to the education community regarding emergency management for education facilities, both public and private. • As a Subsector within the Government Facilities Sector (GFS), works with the GFS to help ensure the Education Subsector gets appropriate attention in steady-state protection efforts, as well as in the incident management environment.

Agency	Functions
Department of Energy	• Serves as the SSA for the Energy Sector. • Maintains the United States continuous and reliable energy supplies through preventive measures as well as supporting restorative actions.
Department of Health and Human Services (HHS)	• Serves as the SSA for the Public Health and Healthcare Sector. • Through the Food and Drug Administration, serves as the SSA for food other than the meat, poultry, and egg products portion of the Food and Agriculture Sector. • Is the primary agency for ESF #8 – Public Health and Medical Services coordinating resources for public health and medical services and serves as a support agency to ESF #6 – Mass Care, Emergency Assistance, Housing, and Human Services.
Department of the Interior (DOI)	• Serves as the SSA for the National Monuments and Icons Sector. • Advises and assists in assessing impacts to natural resources, habitats, wildlife, subsistence uses, public lands, Indian tribal lands, and cultural resources and historic properties.
Department of Justice	Reduces terrorist threats and investigates and prosecutes actual or attempted attacks on, sabotage of, or disruptions to CIKR in collaboration with DHS.
Department of Labor	Through the Occupational Safety and Health Administration, provides worker safety advice, assistance, and policy support for CIKR-related activities.
Department of State	• Works with foreign governments and international organizations to strengthen U.S. CIKR protection efforts. • When requested, provides liaison to USACE in the event of incidents having potential international implications. • In accordance with the International Coordination Support Annex, coordinates international offers of public works and engineering assistance and support.
Department of Transportation (DOT)	• Collaborates with DHS on matters of transportation security and transportation infrastructure protection, and is additionally responsible for operating the National Airspace System. • Collaborates with DHS to regulate transportation of hazardous materials (all modes), including pipelines.
Department of the Treasury	• Serves as the SSA for the Banking and Finance Sector and collaborates with other vital CIKR sectors to foster information sharing regarding cross-sector vulnerabilities and protective measures within the sector. • Assesses incident impact to the Banking and Finance Sector. • Provides expertise on the overall economic impact to CIKR. • Serves as the Primary Economic Advisor to the President.
Department of Veterans Affairs	• Contributes extensive expertise to both the Government Facilities and Public Health and Healthcare Sectors through active participation in its respective GCC. • Serves as a supporting agency for a number of ESFs, providing coordination with the medical system as well as direct resources and support for incident management efforts.
Environmental Protection Agency (EPA)	Serves as the SSA for the Drinking Water and Water Treatment Systems Sector.

Agency	Function
Federal Energy Regulatory Commission	• Regulates interstate transmission of electricity, natural gas, and oil. • As an independent agency, reviews proposals to build liquefied natural gas terminals and interstate natural gas pipelines and licenses hydropower projects. • Through the Office of Dam Safety, regulates approximately 2,100 dams that generate electricity.
The Intelligence Community	• Provides vital service to identify and assess threats that may impact the Nation's CIKR. • With DOD and other appropriate Federal departments, such as DOI and DOT, collaborates with DHS on development and implementation of geospatial programs to map, image, analyze, and sort CIKR data. • Serves as a source of intelligence information necessary for CIKR protection. DHS works with Federal departments and agencies to identify and help protect those positioning, navigation, and timing services that are critical enablers for CIKR sectors. • Collaborates with DHS and other agencies, such as EPA, that manage data addressed by Geographic Information Systems.
Nuclear Regulatory Commission (NRC)	• Ensures the protection of the health and safety of the public or the common defense and security involving the use of NRC-licensed radioactive materials in commercial nuclear reactors for electric power generation and nonpower nuclear reactors for research, testing, and training; medical, industrial, and academic uses of radioactive materials, and facilities that fabricate nuclear fuel; and transportation, storage, and disposal of nuclear materials and waste. • Closely coordinates its actions with its licensees, DHS, other Federal agencies, and State and local government officials during radiological incidents by providing advice, guidance, and support as needed. • Performs independent assessments of incidents and potential offsite consequences and, as appropriate, provides recommendations concerning any protective measures.
Office of Science and Technology Policy	Coordinates with DHS to further interagency research and development related to CIKR protection.
U.S. Postal Service (USPS)	• Serves as a member of the Postal and Shipping Sector Coordinating Council;. • Works in cooperation and collaboration with the DHS Transportation Security Administration, the SSA for the Postal and Shipping Sector. • Collects and reports on damage and disruption to USPS facilities and operations as information becomes available.
Information Sharing and Analysis Center Council	• Supports sector-specific information and/or intelligence requirements for incidents, threats, and vulnerabilities. • Provides secure capabilities for members to exchange and share information on cyber, physical, or other threats. • Establishes and maintains operational-level dialogue with appropriate governmental agencies, identifying and disseminating knowledge and effective practices.
Partnership for Critical Infrastructure Security (PCIS)	Coordinates cross-sector initiatives to support CIKR protection. The PCIS membership is comprised of one or more members and their alternates from each of the CIKR SCCs.
State, Local, Tribal, and Territorial Government Coordinating Council	Coordinates and communicates among State, local, tribal, and territorial homeland security communities to ensure that they are fully integrated in national CIKR protection planning and implementation. The SLTTGCC membership is comprised of senior representatives from State, local, tribal, and territorial agencies including homeland security advisors, decisionmakers, and CIKR stakeholders.

APPENDIX A: SECTOR-SPECIFIC AGENCIES FOR CRITICAL INFRASTRUCTURE AND KEY RESOURCES

The following list includes those Federal departments and agencies identified in HSPD-7 as responsible for CIKR protection activities in specified CIKR sectors.

Table A-1. Sector-Specific Agencies for Critical Infrastructure and Key Resources

Sector-Specific Agency	Critical Infrastructure and Key Resources Sector
Department of Agriculture[20]	Agriculture and Food
Department of Health and Human Services[21]	
Department of Defense[22]	Defense Industrial Base
Department of Energy[23]	Energy
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Water Treatment Systems[24]
Department of Homeland Security	
Office of Infrastructure Protection	Chemical
	Commercial Facilities
	Dams
	Emergency Services
	Nuclear Reactors, Materials, and Waste
Office of Cyber Security and Communications	Information Technology
	Communications
Transportation Security Administration	Postal and Shipping
Transportation Security Administration/U.S. Coast Guard[25]	Transportation Systems[26]
Immigration and Customs Enforcement/Federal Protective Service	Government Facilities

[20] USDA is responsible for agriculture and food (meat, poultry, and egg products).
[21] HHS is responsible for food other than meat, poultry, and egg products.
[22] Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense, including the chain of command for military forces from the President as Commander in Chief, to the Secretary of Defense, to the commander of military forces, or military command and control procedures.
[23] The Energy Sector includes the production, refining, storage, and distribution of oil, gas, and electric power, except for commercial nuclear power facilities.
[24] Drinking Water and Water Treatment Systems includes drinking water supply, treatment, and distribution; and wastewater collection, treatment, and disposal.
[25] DHS/U.S. Coast Guard is the SSA for the maritime transportation mode.
[26] As stated in HSPD-7, DOT and DHS will collaborate on all matters relating to transportation security and transportation infrastructure protection.

APPENDIX B: RELATIONSHIP OF EMERGENCY SUPPORT FUNCTIONS TO CIKR SECTORS

This table shows how the 15 Emergency Support Functions map to the 17 CIKR sectors.

Table B-1. Relationship of Emergency Support Functions to CIKR Sectors

Emergency Support Function	Related CIKR Sectors
ESF Primary Agencies: Coordinate Resources Support and Program Implementation for Response, Recovery, Restoration, and Mitigation programs directly related to incident management functions.	**Sector-Specific Agencies (SSAs)** Coordinate efforts to protect the Nation's CIKR from terrorist attacks and for helping to strengthen preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.
ESF #1 – Transportation **Primary Agency:** Department of Transportation	• **Transportation Systems** **SSA:** DHS/Transportation Security Administration • **Postal and Shipping** **SSA:** DHS/Transportation Security Administration • **Emergency Services** • **SSA:** DHS/Infrastructure Protection
ESF #2 – Communications **Primary Agencies:** DHS/Cybersecurity and Communications/National Communications System DHS/Federal Emergency Management Agency	• **Information Technology** **SSA:** DHS/Cybersecurity and Communications • **Communications** **SSA:** DHS/Cybersecurity and Communications/ National Communications System • **Emergency Services** **SSA:** DHS/Infrastructure Protection
ESF #3 – Public Works and Engineering **Primary Agencies:** DHS/Federal Emergency Management Agency DOD/U.S. Army Corps of Engineers	• **Drinking Water and Water Treatment Systems** **SSA:** Environmental Protection Agency • **Dams** **SSA:** DHS/Infrastructure Protection • **Energy** **SSA:** Department of Energy • **Emergency Services** **SSA:** DHS/Infrastructure Protection • **Government Facilities** **SSA:** DHS/Immigration and Customs Enforcement/ Federal Protective Service • **National Monuments and Icons** **SSA:** Department of the Interior
ESF #4 – Firefighting **Primary Agency:** USDA/Forest Service	• **Emergency Services** **SSA:** DHS/Infrastructure Protection • **Government Facilities** **SSA:** DHS/Immigration and Customs Enforcement/ Federal Protective Service
ESF #5 – Emergency Management **Primary Agency:** DHS/Federal Emergency Management Agency	• **Emergency Services** **SSA:** DHS/Infrastructure Protection • **Government Facilities** **SSA:** DHS/Immigration and Customs Enforcement/ Federal Protective Service

Emergency Support Function	Related CIKR Sectors
ESF #6 – Mass Care, Emergency Assistance, Housing, and Human Services **Primary Agency:** DHS/Federal Emergency Management Agency	• **Emergency Services** **SSA:** DHS/Infrastructure Protection • **Public Health and Healthcare** **SSA:** Department of Health and Human Services
ESF #7 – Logistics Management and Resource Support **Primary Agencies:** General Services Administration DHS/Federal Emergency Management Agency	All
ESF #8 – Public Health and Medical Services **Primary Agency:** Department of Health and Human Services	• **Emergency Services** **SSA:** DHS/Infrastructure Protection • **Public Health and Healthcare** **SSA:** Department of Health and Human Services
ESF #9 – Search and Rescue **Primary Agencies:** DHS/Federal Emergency Management Agency DHS/U.S. Coast Guard DOI/National Park Service DOD/U.S. Air Force	• **Emergency Services** **SSA:** DHS/Infrastructure Protection
ESF #10 – Oil and Hazardous Materials Response **Primary Agencies:** Environmental Protection Agency DHS/U.S. Coast Guard	• **Chemical** **SSA:** DHS/Infrastructure Protection • **Nuclear Reactors, Materials, and Waste** **SSA:** DHS/Infrastructure Protection • **Emergency Services** **SSA:** DHS/Infrastructure Protection
ESF #11 – Agriculture and Natural Resources **Primary Agencies:** Department of Agriculture Department of the Interior	• **Agriculture and Food** **SSA:** Department of Agriculture and Department of Health and Human Services/Food and Drug Administration • **National Monuments and Icons** **SSA:** Department of the Interior
ESF #12 – Energy **Primary Agency:** Department of Energy	• **Energy** **SSA:** Department of Energy • **Nuclear Reactors, Materials, and Waste** **SSA:** DHS/Infrastructure Protection • **Dams** **SSA:** DHS/Infrastructure Protection
ESF #13 – Public Safety and Security **Primary Agency:** Department of Justice	• **Emergency Services** **SSA:** DHS/Infrastructure Protection • **Postal and Shipping** SSA: DHS/Transportation Security Administration • **All others as appropriate**

Emergency Support Function	Related CIKR Sectors
ESF #14 – Long-Term Community Recovery **Primary Agencies:** Department of Agriculture DHS/Federal Emergency Management Agency Department of Housing and Urban Development Small Business Administration	• **Banking and Finance** **SSA:** Department of the Treasury • **Commercial Facilities** **SSA:** DHS/Infrastructure Protection • **Drinking Water and Water Treatment Systems** **SSA:** Environmental Protection Agency
ESF #15 – External Affairs **Primary Agency:** DHS/Federal Emergency Management Agency	**All**

Notes:

- When requested, and upon approval of the Secretary of Defense, DOD provides DSCA during domestic incidents. In the context of the *NRF*, DOD is considered a support agency for all ESFs. DOD is the SSA for the Defense Industrial Base sector, which may have links to many of the ESFs.

- As stated in HSPD-7, DOT and DHS will collaborate on all matters relating to transportation security and transportation infrastructure protection.

List of Acronyms

CFR	Code of Federal Regulations
CIKR	Critical Infrastructure and Key Resources
CII	Critical Infrastructure Information
COP	Common Operating Picture
DHS	Department of Homeland Security
DOD	Department of Defense
DOI	Department of the Interior
DOJ	Department of Justice
DOT	Department of Transportation
DPA	Defense Production Act
DSCA	Defense Support of Civil Authorities
EOC	Emergency Operations Center
EPA	Environmental Protection Agency
ESF	Emergency Support Function
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GCC	Government Coordinating Council
GFS	Government Facilities Sector
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HHS	Department of Health and Human Services
HSAS	Homeland Security Advisory System
HSIN	Homeland Security Information Network
HSPD	Homeland Security Presidential Directive
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
JFO	Joint Field Office
NADB	National Asset Database
NCC	National Coordinating Center for Telecommunications
NCS	National Communications System
NICC	National Infrastructure Coordinating Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NISAC	National Infrastructure Simulation and Analysis Center
NOAA	National Oceanic and Atmospheric Administration
NOC	National Operations Center
NRC	Nuclear Regulatory Commission
NRCC	National Response Coordination Center
NRF	National Response Framework
NS/EP	National Security and Emergency Preparedness
OI&A	Office of Intelligence and Analysis
OIP	Office of Infrastructure Protection
PA	Office of Public Affairs
PCII	Protected Critical Infrastructure Information
PCIS	Partnership for Critical Infrastructure Security
PFO	Principal Federal Official
PSA	Protective Security Advisor
RRCC	Regional Response Coordination Center
SCC	Sector Coordinating Council
SIOC	Strategic Information and Operations Center
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SSA	Sector-Specific Agency
SSP	Sector-Specific Plan
SVA	Security Vulnerability Assessment
USACE	U.S. Army Corps of Engineers
US-CERT	United States Computer Emergency Readiness Team
USDA	Department of Agriculture

This page intentionally left blank.