Supplemental Tool: Connecting to the NICC and NCCIC

Homeland
Security

Connecting to the NICC and the NCCIC

> *There shall be two national critical infrastructure centers operated by DHS – one for physical infrastructure and another for cyber infrastructure. They shall function in an integrated manner and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect the physical and cyber aspects of critical infrastructure.*
>
> *– Presidential Policy Directive 21, Critical Infrastructure Security and Resilience*

Presidential Policy Directive 21 (PPD-21) highlights the role of the national physical and cyber coordinating centers in enabling successful critical infrastructure security and resilience outcomes. The National Infrastructure Coordinating Center (NICC) and the National Cybersecurity and Communications Integration Center (NCCIC) fulfill this Department of Homeland Security (DHS) responsibility within the critical infrastructure partnership. This supplement describes how partners throughout the critical infrastructure community—owners and operators; Federal partners; regional consortia; and State, local, tribal, and territorial governments—can connect to the NICC and NCCIC. It describes the information desired by the centers and their partners, as well as how the centers protect and analyze data to inform prevention, protection, mitigation, response, and recovery activities.

These centers, along with an integrated analysis function, build situational awareness across critical infrastructure sectors based on partner input and provide information with greater depth, breadth, and context than information from any individual partner or sector. PPD-21 highlights the importance of these centers and the multidirectional information sharing that enables them to build true situational awareness. "The success of these national centers, including the integration and analysis function, is dependent on the quality and timeliness of the information and intelligence they receive from the Sector-Specific Agencies (SSAs) and other Federal departments and agencies, as well as from critical infrastructure owners and operators and State, local, tribal, and territorial (SLTT) entities."

1. The Centers

The National Infrastructure Coordinating Center (NICC)

The NICC is the watch center component of the National Protection and Programs Directorate's (NPPD) Office of Infrastructure Protection (IP), the national physical critical infrastructure center designated by the Secretary of Homeland Security, and an element of the National Operations Center (NOC). It is the national focal point for critical infrastructure partners to obtain 24/7 situational awareness and integrated actionable information to secure the Nation's physical critical infrastructure. When an incident or event impacting critical infrastructure occurs that requires coordination between DHS and the owners and operators of critical infrastructure, the NICC is the national coordination hub to support the security and resilience of physical critical infrastructure assets. The NICC collaborates with Federal departments and agencies, SLTT governments, and private sector partners to monitor potential, developing, and current regional and national operations of the Nation's critical infrastructure sectors.

The National Cybersecurity and Communications Integration Center (NCCIC)

The NCCIC is the lead cybersecurity and communications organization within DHS, serving as the national cyber critical infrastructure center designated by the Secretary of Homeland Security. It applies analytic resources; generates shared situational awareness; and coordinates synchronized response, mitigation, and recovery efforts in the event of significant cyber or communications incidents by regularly coordinating with law enforcement, the Intelligence Community (IC), international computer emergency readiness teams, domestic information sharing and analysis centers (ISACs), and critical infrastructure partners to share information and collaboratively respond to incidents.

Information-Sharing Mechanisms

Critical infrastructure owners and operators receive information directly from the centers, but also frequently receive information through their respective SSAs or other parties such as regional consortia, ISACs, fusion centers, etc.

Online Resources (Web portals and Public Internet)

- **Homeland Security Information Network – Critical Infrastructure (HSIN-CI):** HSIN-CI provides secure networked information sharing covering the full range of critical infrastructure interests. Validated critical infrastructure partners can access HSIN-CI.
  - The NICC posts content on HSIN-CI from a variety of internal and external sources that is available to all critical infrastructure partners, including incident situation reports, threat reports, impact modeling and analysis, common vulnerabilities, potential indicators, and protective measures.
  - The NICC combines current high-interest incidents and events on the HSIN-CI "front page," providing easy access to relevant information.
  - Individual sectors and subsectors self-manage more specific portals within HSIN-CI where smaller communities of participants receive and share relevant information for their particular information needs.
  - HSIN-CI also can facilitate multiple types of information sharing and coordination, including suspicious activity reporting, webinars, shared calendars, etc.

  - To ensure broad sharing of essential information, the NICC also receives and provides information via other HSIN portals.

- **United States Computer Emergency Readiness Team (US-CERT) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) portal:** The NCCIC provides a secure, Web-based, collaborative system to share sensitive cybersecurity prevention, protection, mitigation, response, and recovery information with validated private sector, government, and international partners. It gives partners access to two components of the secure portal, which hold information regarding cyber indicators, incidents, and malware digests for critical infrastructure systems:
  - The Cobalt Compartment is an information hub for enterprise systems security.
  - The Control System Compartment provides material on industrial control systems, limited to control system asset owners and operators.
- **The US-CERT.gov Web site** provides extensive vulnerability and mitigation information to partners around the world, including:
  - A control systems section containing Control Systems Advisories and reports of particular interest to critical infrastructure owners and operators.
  - A National Cyber Awareness System, which provides timely alerts, bulletins, tips, and technical documents to those who sign up.
  - Cybersecurity incident reporting, providing critical infrastructure partners with a secure means to report cybersecurity incidents.

Email and Other Electronic Means

Both centers maintain connectivity with a variety of partners through email, automated data exchange, and other means. This allows for very precise outreach when broad communication is inappropriate or not possible. In coordination with the SSAs, other departments and agencies, and the law enforcement community, both the NICC and the NCCIC will reach out directly to specific partners as a developing situation or information need evolves. Similarly, both centers are available to stakeholders throughout the partnership when a rapid response is essential.

Teleconferences

- National threat briefings: During periods of heightened threat or concern, the NICC will coordinate through the SSAs and relevant critical infrastructure partners to conduct unclassified teleconferences regarding current intelligence, expected actions, and protective measure options for consideration.

- Incident-specific cross-sector calls:
  - NICC: During significant incidents, the NICC will coordinate calls with the SSA and Government Coordinating Council (GCC)/Sector Coordinating Council (SCC) leadership to discuss national and cascading impacts and determine potential actions to mitigate risk. If necessary, the NICC will also conduct large-scale teleconferences with locally affected partners and share mutual situational awareness and address key areas of concern.
  - NCCIC: The NCCIC will similarly reach out to sector partners through its established mechanisms.

Classified Meetings and Briefings

- During periods of heightened threat or concern with significant classified components, the NICC and/or NCCIC, in conjunction with the IC, will coordinate with SSAs, GCCs, and SCCs and conduct classified briefings on current intelligence, expected actions, and protective measure options for consideration.
- The centers, in collaboration with SSAs and the IC, may assist in arranging similar briefings outside of the National Capital Region.

In-Person Meetings and Regional Extensions

- Onsite consultations and self-evaluations: The NCCIC helps asset owners prepare for and protect from cyber attacks, via no-cost, onsite, defense-in-depth cybersecurity strategic analysis of critical infrastructure by DHS subject matter experts.
- IP regional staff: The NICC works closely with DHS and IP field personnel and other regional public and private partners. It works with DHS Protective Security Advisors and Chemical Security Inspectors in the field to prevent information stove pipes and reduce duplicative efforts.

Integrating Partners into Daily Operations

The NICC and NCCIC incorporate critical infrastructure partners, including ISACs, SSAs, and Federal law enforcement, into their day-to-day operations, including housing both public and private sector partners in their physical watch facilities, as appropriate. These partners serve as bidirectional conduits of information between the centers and the liaison's home agency or sector.

2. Federal Partners

Both centers maintain active relationships with Federal partners, such as SSAs, law enforcement, and emergency management communities. Other government agencies also work with the NICC and NCCIC and share interest in critical infrastructure-related information. For example, the NICC works closely with the State Department's Overseas Security Advisory Council, which provides information regarding threats to physical infrastructure overseas to American organizations and can ensure this information is available to the domestic critical infrastructure community. At the same time, the NCCIC works on a daily basis with other Federal cyber centers to exchange critical information and coordinate analytical and response processes. Both centers provide reports to the NOC to facilitate shared situational awareness across the Federal community.

Sector-Specific Agencies

The SSAs actively engage with the centers and other entities, consistent with statutory authority and other appropriate policies, directives, or regulations. The centers rely on the SSAs and Emergency Support Function (ESF) structure of the National Response Framework to ensure connectivity broadly across the sectors. During significant incidents, the SSAs provide the NICC and NCCIC with sector impacts for inclusion in the comprehensive infrastructure Common Operating Picture (COP), which is then shared with the SSAs and other partners, as well as with Federal partners and entities engaged in international efforts—including the Department of State, responsible for engaging foreign governments, the U.S. private sector operating overseas, and international organizations—to strengthen the security and resilience of critical infrastructure located outside the United States.

The Intelligence Community

The NICC and NCCIC serve as a major conduit for IC threat information—both classified and unclassified—to the owners and operators of critical infrastructure.

Federal Law Enforcement

The NICC and NCCIC, within their information-sharing protocols and protections, provide suspicious activity reporting and other similar information to Federal law enforcement entities.

Federal Emergency Management

During major incidents, the NICC and NCCIC closely coordinate with the Federal Emergency Management Agency (FEMA) to ensure that overall critical infrastructure status and impacts on life and safety are understood throughout the Federal incident response community. Both the NICC and NCCIC provide liaisons directly to the National Response Coordination Center to ensure continuous bidirectional information flow. The SSAs are often directly tied to the Federal emergency management structure through the ESFs, as noted in Table 1, and provide detailed sector-specific status information, while the NICC and NCCIC provide the cross-sector analysis of the system-of-systems that makes up our national critical infrastructure. During major national incidents, particular focus is placed on those lifeline functions on which most critical infrastructure sectors depend, which are communications, energy, transportation, and water. The Critical Infrastructure Support Annex to the National Response Framework provides more detail on critical infrastructure information sharing during significant incidents.

Table 1 - Sector-Specific Agencies and Related Emergency Support Functions

Critical Infrastructure Sector	Sector Specific Agency	Related Emergency Support Function(s) (ESF)[1]
Chemical	Department of Homeland Security	
Commercial Facilities		
Communications		ESF #2 – Communications (coordinator/primary)
Critical Manufacturing		
Dams		ESF #3 – Public Works and Engineering (support)
Emergency Services		ESF #4 – Firefighting (support) ESF #5 – Information and Planning (support) ESF #13 – Public Safety and Security (support)
Information Technology		
Nuclear Reactors, Materials & Waste		ESF #12 – Energy (coordinator/primary)
Food & Agriculture	Department of Agriculture, Department of Health and Human Services	ESF #11 – Agriculture and Natural Resources (USDA: (coordinator/primary; HHS: support)
Defense Industrial Base	Department of Defense	
Energy	Department of Energy	ESF #12 – Energy (coordinator/primary) ESF #10 – Oil and Hazardous Materials Response (support)
Healthcare & Public Health	Department of Health and Human Services	ESF #6 – Mass Care, Emergency Assistance, Housing, and Human Services (support) ESF #8 – Public Health and Medical Services (coordinator/primary)
Financial Services	Department of the Treasury	
Water & Wastewater Systems	Environmental Protection Agency	ESF #3 – Public Works and Engineering (support)
Government Facilities	Department of Homeland Security, General Services Administration	
Transportation Systems	Department of Homeland Security, Department of Transportation	ESF #1 – Transportation (DOT: coordinator/primary; DHS: support)

[1] The ESFs provide the structure for coordinating Federal interagency support for a Federal response to an incident. They are mechanisms for grouping functions most frequently used to provide Federal support to States and Federal-to-Federal support, both for declared disasters and emergencies under the Stafford Act and for non-Stafford Act incidents. This table is meant to provide information on various ESF responsibilities of the SSAs; it is not an exhaustive list of ESF responsibilities for the Federal departments and agencies listed.

3. Critical Infrastructure Owners and Operators

Individual critical infrastructure owners and operators will often send and receive information to and from the national centers through intermediary entities, but can always reach the centers directly if necessary to share or request mission-critical information. The centers are in continuous contact with the ISACs and SSAs.

4. SLTT Government Partners, Regional Partnerships and Consortia

Public and private sector owners and operators of critical infrastructure and other non-Federal entities may consult with the NICC and NCCIC as resources for government and regional public-private consortia and coalitions. The coordinating centers may leverage regional or other partnerships for information on critical infrastructure, especially during significant incidents affecting sectors within a region. The centers, in conjunction with the ESF structure and other Federal authorities, where appropriate, also share information with other entities (e.g., State and major urban area fusion centers, InfraGard chapters, Area Maritime Security Committees, and FEMA regional offices).

5. Common Information-Sharing Requirements, Systems, and Processes

The two centers continuously set and refine common information-sharing requirements, systems, and processes to facilitate a COP that delivers actionable information to decision makers at all levels. Specifically:

- **Refine and manage critical information requirements:** To build situational awareness, each center operates using a set of defined critical information requirements (CIRs), which they should continuously evaluate and refine. SSAs and other departments and agencies may augment these with sector-specific CIRs. The centers coordinate these requirements with critical infrastructure owners and operators and the SLTTGCC.

- **Leverage the DHS COP for a combined, cross-sector situational awareness picture for critical infrastructure security and resilience:** The centers create data feeds and Web services across SSAs and other Federal and SLTT governments, as well as private sector entities to inform the critical infrastructure centers and overall critical infrastructure COP. In turn, the partnership shares this larger national situational awareness picture so participants have greater depth and context of knowledge than they would otherwise have.

6. Information Protection

The NICC and NCCIC, as information management and coordination centers, are capable of handling information under a wide range of caveats, including, but not limited to classified, For Official Use Only, Personally Identifiable Information (PII), Sensitive PII, Protected Critical Infrastructure Information, Chemical-terrorism Vulnerability Information, Law Enforcement Sensitive, and various industry standards (e.g., the Traffic Light Protocol used by many ISACs).

7. Get Connected

Centers

National Infrastructure Coordinating Center:
nicc@hq.dhs.gov
202–282–9201

National Cybersecurity and Communications Integration Center:
nccic@hq.dhs.gov
888–282–0870

Portals

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

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

For questions regarding HSIN-CI access, please contact the NICC.

US-CERT and ICS-CERT Portal:
To request access to the Cobalt Compartment, send an email to NCCIC_Partnership@hq.dhs.gov with the subject line, "Request access to Cobalt Compartment." To access the Control System Compartment, send an email to NCCIC_Partnership@hq.dhs.gov with the subject line, "Request access to Control System Compartment."

To qualify for either compartment, a requestor must:

- Be a U.S.-based organization
- Have a role within an organization's network defense community
- Be a control system asset owner/operator (specific to the Control System Compartment)

Homeland
Security