IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

NATIONAL CRITICAL FUNCTIONS

Access to electricity, transportation, the internet, and a myriad of other services are of paramount importance to the Nation's societal and economic well-being. Each day, critical infrastructure operations ensure that **National Critical Functions (NCFs)**, which serve as the operational backbone for modern society, are running. The NCFs are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

The **Cybersecurity and Infrastructure Security Agency (CISA)**, through the **National Risk Management Center (NRMC)**, works with government and industry partners to identify and manage risks to the NCFs in a targeted, prioritized, and strategic manner to improve the resilience across the Nation's critical infrastructure.

NCF OVERVIEW

Technological advances and hyperconnectivity have improved critical infrastructure operations and transformed the Nation's 16 critical infrastructure sectors into a complex, interconnected ecosystem. At the same time, the integration of information and operational technologies and the complexity of supply chains has created new vectors through which adversaries can exploit vulnerabilities in assets, systems, and networks that enable America's economic competitiveness and national security. Examples of NCFs include electricity generation that powers homes and businesses, transportation of commodities and people, and access to GPS data for cellular networks. An interruption to one NCF can have cascading consequences across industries and society.

On April 30, 2019, CISA published a set of 55 NCFs. The effort was led by CISA's NRMC in coordination with government and private sector partners, industry experts, and other stakeholders to identify what functions are so vital that, if disrupted or sabotaged, may cause cross-sector impacts or nationwide degradation. The set of NCFs are organized into four areas:

Connect	Connections by technologies that enable critical communications and capabilities to send and receive data (e.g., internet connectivity and satellite access)
Distribute	Distribution methods that allow the movement of goods, people, and utilities inside and outside the United States (e.g., electricity distribution and cargo transportation)
Manage	Management processes that ensure our national security and public health and safety (e.g., managing hazardous material, conducting elections, and national emergencies)
Supply	Supplies of materials, goods, and services that secure our economy (e.g., water and housing)

NCF FRAMEWORK: CROSS-SECTOR RISK MANAGEMENT

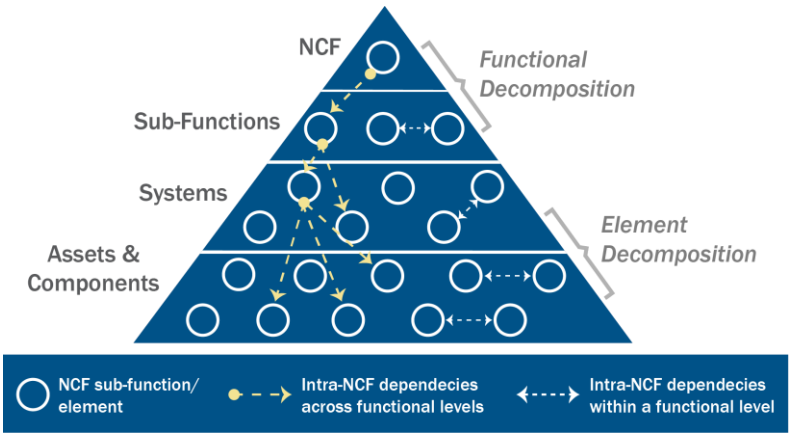
The NCF Framework transforms the perspective of managing risk from the entity level (assets and organizations) to understanding how entities come together to provide services and functions. This framework incorporates sector expertise to understand the key assets, systems, and networks that contribute to each NCF. Since a majority of critical infrastructure is privately-owned, effective risk management depends on information sharing between the private sector and government and collaboration across sectors to understand, as completely as possible, the systemic risk picture that the consequences of a threat—cyber, physical, technological, or natural—can have on NCFs.

By viewing risk through a functional lens, the critical infrastructure community can identify where key dependencies and interdependencies lie between cyber and physical systems, as well as between NCFs. For example, if the electric grid is knocked offline, water and wastewater systems cannot provide clean water, natural gas cannot flow to provide heat, and telecommunications systems may become inoperative if backup power sources fail. The NCF Framework improves the community's ability to manage previously identified risks and provides the foundation for identifying new pockets of risk that need to be managed.

DEEPENING UNDERSTANDING OF CRITICAL INFRASTRUCTURE RISK

In the year following the publication of the NCFs, the NRMC has defined each of the 55 NCFs and built a baseline understanding of the systems and technologies involved in their operations. The NRMC will continue to mature the NCF Framework by increasing the depth of understanding how NCFs operate, and analyzing the community of stakeholders relevant to each NCF. This understanding will inform the ongoing development of an NCF Risk Architecture.

This architecture—a technology-enabled analytic tool—will break down each NCF into its sub-functions and lower-level activities to enable CISA to quickly evaluate, identify, and assess both operational and strategic risks to the Nation's infrastructure. Through engagement with partners and industry, the NRMC will develop the NCF Risk Architecture through the following activities:



1. Functionally decompose NCF to understand contributing functional elements,
2. Link assets to sub-functions,
3. Identify data sources that relate to assets,
4. Qualitatively link sub-functions of NCF to NCF dependencies using the NCF definitions,
5. Analyze the directionality of NCF to NCF interdependencies.

Additionally, the NRMC will work with NCF stakeholders to support development of an NCF Risk Register to identify priority risks and organize activities that government and industry are undertaking to address critical infrastructure risks.

It is important to understand that the NCF Risk Register is not meant to be static. As new risks emerge—such as the consequences of disinformation and foreign influence activities on public confidence during elections or COVID-19 response efforts—CISA will continue to assist with policy, doctrine, and process enhancements and additional analysis to reprioritize or identify new priorities and establish risk management initiatives to effectively secure the Nation.

NCF RESOURCES

- National Critical Functions: cisa.gov/national-critical-functions
- NCF Set: cisa.gov/national-critical-functions-set
- NCF Status Update to the Critical Infrastructure Community: cisa.gov/publication/ncf-status-update
- NRMC Resources: cisa.gov/nrmc-resources

For questions or to seek additional help, contact us at NCF@hq.dhs.gov.