



December 15, 2021

MEMORANDUM FOR DISTRIBUTION

FROM: Bob Kolasky 
Assistant Director, CISA
National Risk Management Center

SUBJECT: **Status Update on the National Critical Functions**

Critical Infrastructure Colleagues—

In the Spring of 2019, the Cybersecurity and Infrastructure Security Agency (CISA) published the first set of National Critical Functions (NCFs). We want to thank you for your continued support in helping CISA advance the NCFs as a national-level risk management framework, in addition to helping us better understand the criticality of the NCFs across the critical infrastructure sectors. Over the past 12 months, we have made significant progress with the NCFs, and would like to provide the critical infrastructure community with an overview on what we have done and where we would like to go moving forward to enhance our Nation's critical infrastructure risk management capabilities.

The 55 NCFs represent a foundational shift that enable the identification and prioritization of systemic risk to critical infrastructure by focusing on the functions, the key assets, systems, and networks that support them, as well as the critical technologies and dependencies that enable them. The NCF Framework is based on the idea that critical infrastructure is increasingly cross-sector, and that a siloed approach is not sufficient to manage risk, particularly around cybersecurity.

CISA's National Risk Management Center (NRMC) uses the NCFs to support national-level risk prioritization and governance. The attached paper talks through how we do that and what progress we have made in our ability to do so in 2021.

As we move forward, the NRMC will continue to further mature, refine, and operationalize the NCF Framework to identify, prioritize, and mitigate national level risks in partnership with the Federal Senior Leadership Council (FSLC) and critical infrastructure partners. This will include informing and reinforcing CISA priorities and strategic mitigation capabilities like the Joint Cyber Defense Collaborative (JCDC).

We welcome any feedback and encourage sector partners to reach out to the NCF team at ncf@hq.dhs.gov to receive feedback on the NCF status update or to get involved in these efforts.

Attachment: "National Critical Functions: Status Update to the Critical Infrastructure Community"

Distribution:

- Federal Senior Leadership Council Members
- Leadership of the Critical Infrastructure Partnership Advisory Council



National Critical Functions

Status Update to the Critical Infrastructure Community

December 2021

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



“It is the policy of my Administration to safeguard the critical infrastructure of the Nation, with a particular focus on the cybersecurity and resilience of systems supporting National Critical Functions, defined as 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 national security, economic security, public health or safety, or any combination thereof.”

*President Joseph R. Biden,
National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems,
July 28, 2021*



INTRODUCTION

Generating electricity, operating core communications networks, supplying water, conducting elections, and a myriad of other critical functions are vital to national security, economic competitiveness, community well-being, and public confidence. In the face of rapidly evolving cyber and other risk environments, presidential policy has affirmed the importance of secure and resilient National Critical Functions (NCFs).

To support that goal, the Cybersecurity and Infrastructure Security Agency's (CISA) National Risk Management Center (NRMC) has developed the NCF Risk Management Framework to analyze and manage the risks to our Nation's critical infrastructure. The NCF Framework uses an asset-centric approach to better assess how failures in key systems, assets, components, and technologies may cascade across sectors, and the overall impacts to the Nation. It enables a richer understanding of how entities—such as electric facilities, banks, communications hubs, and managed service providers—come together to produce critical functions. Building off the critical infrastructure risk management framework established in the [National Infrastructure Protection Plan](#), this risk management approach addresses cross-cutting risks that affect multiple sectors and industries.

The NCF Framework uses the [55 NCFs](#) as a basis to identify and analyze critical infrastructure risk. This allows for a unified community-wide perspective for critical infrastructure, and safely and securely delivering those functions is a national security imperative. This risk basis is useful for a common approach to all-hazards risk management and supports prioritization decisions for security and resilience across a range of issues. In times of crisis, when risks from cyberattacks, hurricanes, and terrorist attacks manifest, the NCF Framework helps better target risk response and mitigation efforts that will support the greatest reduction in risks to national security, economic security, public health and safety, and public confidence.

Ultimately, critical infrastructure safety and security depends on a shared effort. By collaborating and partnering with other Federal agencies and the broader critical infrastructure community, we can work together to keep the lights on, the water running, and global data flowing.

The rest of this paper provides an update on the progress that the NRMC has made in building and utilizing the NCF Risk Management Framework.

What are National Critical Functions?

National Critical Functions 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.

Why National Critical Functions?

Effective risk management depends on the critical infrastructure community's ability to engage across sectors to facilitate a shared understanding of risk and integrate a wide range of activities to manage risk. The NCF Framework recognizes:

Critical infrastructure is increasingly cross-sector in nature and a siloed approach, particularly around cybersecurity, is no longer sufficient to manage risk.

Our understanding of risk must evolve from a static asset or organization view to a more holistic approach that focuses on functions and services.

Understanding and mitigating nation-level risks requires more nuanced data collection and analysis methods.

Our need to broaden the stakeholder community involved in critical infrastructure risk management by better engaging non-traditional groups.



ADVANCEMENT IN UNDERSTANDING OF THE NCFs

The 55 National Critical Functions are listed below:

CONNECT 	DISTRIBUTE 	MANAGE 	SUPPLY 
<ul style="list-style-type: none"> ▪ Operate Core Network ▪ Provide Cable Access Network Services ▪ Provide Internet Based Content, Information, and Communication Services ▪ Provide Internet Routing, Access and Connection Services ▪ Provide Positioning, Navigation, and Timing Services ▪ Provide Radio Broadcast Access Network Services ▪ Provide Satellite Access Network Services ▪ Provide Wireless Access Network Services ▪ Provide Wireline Access Network Services 	<ul style="list-style-type: none"> ▪ Distribute Electricity ▪ Maintain Supply Chains ▪ Transmit Electricity ▪ Transport Cargo and Passengers by Air ▪ Transport Cargo and Passengers by Rail ▪ Transport Cargo and Passengers by Road ▪ Transport Cargo and Passengers by Vessel ▪ Transport Materials by Pipeline ▪ Transport Passengers by Mass Transit 	<ul style="list-style-type: none"> ▪ Conduct Elections ▪ Develop and Maintain Public Works and Services ▪ Educate and Train ▪ Enforce Law ▪ Maintain Access to Medical Records ▪ Manage Hazardous Materials ▪ Manage Wastewater ▪ Operate Government ▪ Perform Cyber Incident Management Capabilities ▪ Prepare For and Manage Emergencies ▪ Preserve Constitutional Rights ▪ Protect Sensitive Information ▪ Provide and Maintain Infrastructure ▪ Provide Capital Markets and Investment Activities ▪ Provide Consumer and Commercial Banking Services ▪ Provide Funding and Liquidity Services ▪ Provide Identity Management and Associated Trust Support Services ▪ Provide Insurance Services ▪ Provide Medical Care ▪ Provide Payment, Clearing, and Settlement Services ▪ Provide Public Safety ▪ Provide Wholesale Funding ▪ Store Fuel and Maintain Reserves ▪ Support Community Health 	<ul style="list-style-type: none"> ▪ Exploration and Extraction Of Fuels ▪ Fuel Refining and Processing Fuels ▪ Generate Electricity ▪ Manufacture Equipment ▪ Produce and Provide Agricultural Products and Services ▪ Produce and Provide Human and Animal Food Products and Services ▪ Produce Chemicals ▪ Provide Metals and Materials ▪ Provide Housing ▪ Provide Information Technology Products and Services ▪ Provide Materiel and Operational Support to Defense ▪ Research and Development ▪ Supply Water

Since 2019, the NRMCM has worked to better understand the processes, systems, technologies, and governance that support or enable the provision of each of the 55 NCFs. This process, called functional decomposition, enables a deeper understanding of how entities come together to produce critical functions. The decomposition identifies all the layers (sub-functions, systems, processes, technologies, assets, components, and governance) that produce or deliver an NCF, as well as numerous dependencies and interdependencies within and across each NCF.

Over the last year, the NRMCM worked with interagency and industry partners to identify the sub-functions involved in each of the NCFs, ensuring their valuable insights, data, and feedback informed this process. In 2021, all 55 NCFs were decomposed to the primary and secondary sub-function levels. Currently, the NRMCM is working with the interagency and private sector partners to validate the decompositions.

To date, the NRMCM's decomposition work has identified 294 primary sub-functions and 1,059 secondary sub-functions. In many instances, the NRMCM has decomposed NCFs even further with overall, 3,319 sub-functions having been identified across all 55 NCFs.

To accomplish this decomposition work, the NRMCM is working with Sector Risk Management Agencies and Sector Coordinating Councils to create NCF Communities of Interest around NCFs and actively share these reports with our partners.

This more nuanced understanding helps identify where failures might occur and may point to sustainable risk reduction solutions. Applying this approach to the Nation's critical functions helps the NRMCM identify dependencies and support the resilience of NCFs in a more targeted, prioritized, and strategic manner.

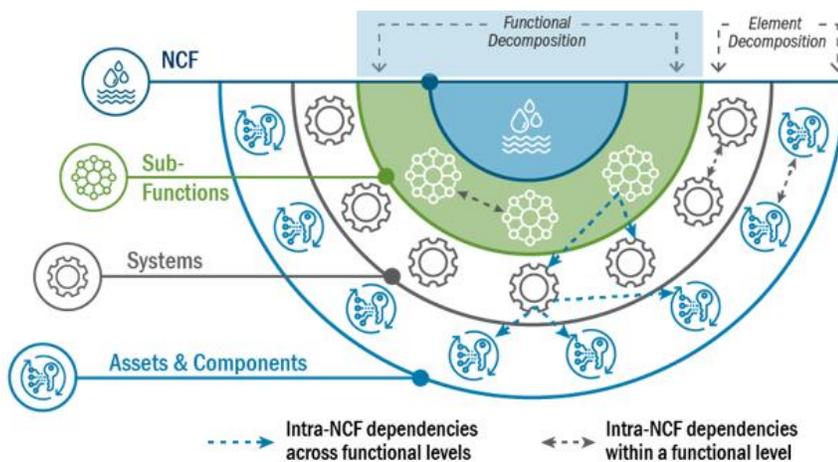


Figure 1: Illustrative example of National Critical Functions Decomposition

NCF UTILITY BY THE NATIONAL RISK MANAGEMENT CENTER

The NRMCM uses the NCFs as a framework and reference point for where it should focus critical infrastructure risk assessment. Below are six categories risk assessments that NRMCM performs, although the NCFs may be used in other contexts as well.

1. **Setting strategic priorities across NCFs for further risk analysis, or risk mitigation.** The principal mechanism for doing this is through the NCF Risk Register. The NCF Risk Register provides a scenario-informed lens in identifying the most critical risks to critical infrastructure. This helps answer the question: *What is the relative level of risk to the NCFs?*
2. **Setting priorities within NCFs for risk mitigation.** The principal mechanism for doing this within NRMCM is via initiatives (e.g., the Election Security Initiative). This helps answer the question: *Where should we focus risk reduction efforts for a specific NCF?*
3. **Criticality assessments and identifying priority infrastructure, technology, or resources.** Examples include supply chain criticality work and the Infrastructure of Concern lists¹. This helps answer the question: *What assets, systems, entities, components, etc., are most critical to the provision of NCFs?*
4. **Threat- or hazard-specific risk analysis.** The NRMCM has done this for potential electromagnetic pulse attacks and is doing it for hazards associated with climate change. This helps answer the question: *Which NCFs are most susceptible to a specific threat or hazard?*
5. **Setting outreach and operational risk management priorities.** The NRMCM did this most prominently for COVID-19, but have supported other incidents and vulnerability management activities, particularly around cyber vulnerabilities. This helps answer the question: *Where should incident response or vulnerability management efforts be focused?*
6. **Assessing the impacts of emerging technologies or technology transition.** The NRMCM is doing this work in the 5G arena and around post-quantum algorithms. This helps answer the questions: *How will emerging technologies change the risk to NCFs? And, which NCFs are at most risk?*

¹ The Infrastructure of Concern (IOC) is an incident-specific, prioritized list of infrastructure assets identified as most likely to be impacted by a particular manmade or natural incident and where disruption would result in the greatest impacts from threats and hazards. The IOC is developed by the NRMCM and used by CISA leadership and regional personnel and stakeholders to support decision-making.



NCF RISK ASSESSMENT APPROACH

The ability to assess risk cohesively and consistently requires a set of concepts and terminology that are foundational and common among the six categories of risk assessments listed, and which also enable information to be shared between them, when appropriate. To support that ability, the NRMC is developing the Risk Architecture. The Risk Architecture is NRMC's technology-enabled tool that will integrate the decomposition data and various other data structures to run analytical models and simulations, and to perform geospatial and calculated analyses to support NCF risk analysis and assessment.

Depending on the circumstances and available information, risks to NCFs may be identified by information about threats and hazards, vulnerabilities, or consequences depending on the circumstances and available information.

Unless explicitly stated, NCF risk assessments address risk to the Nation from a national security, economic security, and public safety perspective, which may be significantly different than the risk to an entity, stakeholder group, or jurisdiction. This is also importantly different from the geographic or sector extent of a vulnerability, or the consequence of a particular scenario. A nationally significant risk may need collaborative mitigation even when a single incident would only have local or regional impacts. That being said, the country's tolerance for risks to NCFs is often far below nation-wide impacts.

Risk may disproportionately impact a particular geographic area. Also, conditions in a constrained geographic area may rise to the level of national significance or may cascade through the Nation. For these reasons, conditions in cities, counties, states, and regions are an important part of understanding NCFs and their risks. The NRMC works with state, local, tribal, territorial, and regional stakeholders to understand the important ways in which these jurisdictions contribute to NCFs and the ways in which they may be disproportionately at risk. The resilience of NCFs depends on a shared effort by infrastructure and communities throughout the country and in some cases, beyond our borders.

Threats and Hazards

The NRMC consistently examines the evolving cyber and other risk environments to identify threats and hazards that could cause a nationally significant impact to NCFs. Threats and hazards can be identified by policy, leadership direction, or analytic methods. The NRMC currently includes the following strategic areas of risk in the NCF Risk Register and considers these in the development of its Risk Architecture:

- Cyber attacks
- Supply chain
- Mis-, dis- and malinformation
- Natural hazards and climate change
- Pandemics
- Terrorism

Scenarios within these strategic risk areas are often used to support risk assessment and management. For example, ransomware is a scenario in the cyber-attack strategic risk area important for assessment and planning in the current risk environment. When supporting operational planning through exercises and other preparedness activities, more specific scenarios are often used, such as a particular strain of ransomware or a hurricane of a specific strength and direction making landfall at a particular place. Likewise, when identifying outreach priorities following the discovery of a cyber vulnerability, more granular cyber scenarios relevant to that vulnerability are needed to evaluate the potential for disruption and harm across multiple NCFs.

During incidents, the threat or hazard is often known, and the assessment focuses on vulnerability and consequences. In 2020 and 2021, NRMC published NCF risk assessments for a pandemic, wildfires, cyber-attacks, hurricanes, and other incidents.



All NCF risk assessments clearly state what threats and hazards are being addressed and how they were selected, as well as any scenarios used as the basis of judgements or estimates of threat, or vulnerability and consequence. Judgements about the likelihood of threats and hazards for NCF assessments are developed with the methods discussed in the [DHS Risk Management Fundamentals](#) and generally rely on evidence about adversary intent and capability or frequency and/or trend data regarding threats or hazards, which can be applied in a variety of methods to assess likelihood.

Vulnerabilities

For there to be a nationally significant risk to an NCF, there must be a characteristic of the function that could lead to a significant consequence. An assessment of vulnerabilities considers system weaknesses as well as exposure and underlying resilience of the function. Examples of NCF vulnerabilities that could lead to nationally significant consequences are provided below. More than one vulnerability may contribute to impacts for a given threat or hazard.

- Chronic underinvestment
- Dependence on a common technology
- Dependence on a scarce good or resource
- Foreign dependence
- Geographic concentration of infrastructure
- High dependence on public trust
- Poor cyber hygiene
- Provision by few entities
- Single points of failure
- Skilled labor dependence
- System interconnectedness
- Unmanaged complexity
- Unrestricted digital access
- Unrestricted physical access

The identification of vulnerabilities is not only important to characterizing risk but also to identifying ways to reduce risk. Vulnerability-reducing investments may have risk reduction value for multiple threats and hazards across multiple NCFs. In such cases, it is often useful to identify a set of NCFs assessed to be most at risk from the vulnerability which can focus the effort to develop mitigation options and identify stakeholders for priority engagement.

In strategic risk assessments where the objective is to characterize an NCF vulnerability to an undesired outcome (consequence), it is also helpful to characterize the degree to which a vulnerability is influencing the likelihood of the undesired outcome. Each vulnerability characteristic has a different measure of degree. For strategic risk assessments, the geographic extent of the vulnerability may be useful information. For example, if we observe poor cyber hygiene in potable water treatment plants throughout the country, the geographic extent of the vulnerability would be national, although the impacts from a single incident may be local. The geographic extent of an NCF vulnerability may be different than the geographic extent of the consequences for a single planning scenario.

Another way to characterize the degree of vulnerability, particularly about dependence on technology or materials, is pervasiveness. For example, if all semiconductor manufacturing plants rely on the same material to make their product, the pervasiveness of that dependence is very high. Likewise, if many natural gas compressor stations rely on pumps provided by a single manufacturer, that is also important evidence about the degree to which that NCF is vulnerable to a disruption or harm from dependence on that pump. Some materials and technologies are used by multiple NCFs. In such cases, the pervasiveness across multiple NCFs must be considered to understand national risk. For example, certain operating systems are used to deliver most NCFs, and some industrial control systems components are used commonly across multiple NCFs.

Consequences

Assessing NCF consequences generally begins with assessing the level of impact of an incident or scenario to the NCF and its ability to function as designed in a safe manner. Based on understanding the degree of



functional degradation, it is possible to assess the broader impact from a degraded NCF.

The [DHS Risk Lexicon](#) notes, “consequence is commonly measured in four ways: human, economic, mission, and psychological, but may also include other factors such as impact on the environment.” NCF risk assessments connect functional degradation to potential impact across these four consequence types. Each consequence type has multiple metrics that can be used to describe the magnitude of the impact, such as fatalities, injuries, and illness for human consequences. Likewise, consequences can be measured in terms of direct impacts or indirect and cascading impacts, as well as how the consequences occur and timeframes.

Other attributes of direct and indirect effects that may be considered include:

- Geographic extent – the spatial extent of the effects
- Population exposure – the number of people affected
- Business exposure – the number and types of businesses affected
- Impact timeframe – how long it takes for the consequences to occur
- Recovery timeframe – how long it takes for the NCF function to return to an acceptable level
- Scalability – if the consequence could occur repeatedly due to a shared vulnerability
- Equity – if some parties are disproportionately impacted by a risk

Evidence and assessment of these consequence features are included in consequence assessments when they are important to support comparisons, decisions, or coordination.

Many NCFs could have failures that include both disruption or degradation of the function and direct harm. A refinery could potentially fail in an event that both stopped the refinery from producing fuel but also directly caused harm such as fatalities, injuries, destruction of property, and environmental impacts. Consequence thresholds can be set for the metrics associated with the consequence types (human, economic, mission, psychological, or environmental), and can also be set based on performance metrics specific to the function. For example, we could say that we are concerned about electricity distribution disruptions causing over 500 million dollars in business interruption (economic consequence) or we could use a metric specific to the function such as 100,000 customers without power more than 48 hours (functional threshold).

Consequences to NCFs can also manifest themselves in lack of confidence in the integrity of the function, which may have nothing to do with the underlying effectiveness of the function itself, but instead the public’s trust as to whether it is working as designed.

When consequences drive risk identification, we start with the question, “what outcome can we not tolerate?” or “what performance level must an NCF achieve?” Once those outcomes are identified, they can support a thorough and systematic examination of the threats, hazards, and vulnerabilities that could lead to those unacceptable outcomes.

NCF RISK GOVERNANCE

To lead federal implementation of the NCF Framework, the Federal Risk Management Working Group was established within the Federal Senior Leadership Council (FSLC); a cross-sector council composed of federal departments and agencies with responsibility in critical infrastructure security and resilience. The Working Group is comprised of interagency representatives who will help coordinate interagency efforts to support CISA and FSLC decision-making for NCF risk identification, analysis, prioritization, and mitigation. To aid risk management prioritization, the Working Group will also support interagency input into the Risk Architecture to compare risk scenarios based on likelihood, vulnerability, and consequence.

CISA is also working to update the National Infrastructure Protection Plan to reflect the NCF Framework. The update will further the goal of breaking down organizational silos through identification, prioritization, and reduction of shared risks. Since a majority of critical infrastructure is privately-owned, effective risk



management depends on private sector and government collaboration to understand systemic risk, and how threats may impact one or more NCFs. This evolution enables the critical infrastructure community to understand and manage the most significant risks facing the Nation.

THE PATH FORWARD

Going forward, the NRMCM will continue to:

- Evolve the NCF Framework in conjunction with interagency and industry partners. Once the NCFs are broken down to the sub-function level, the NRMCM will further breakdown NCFs into their constituent systems, assets, and components to characterize the NCFs more completely and answer specific analytic questions. As with the sub-function decomposition phase, the NRMCM will work closely with its partners to validate accuracy and ensure stakeholder needs are met.
- Expand understanding of the Communities of Interest that surround each NCF.
- Align existing and future NRMCM initiatives, and broader CISA programs, to the NCF Framework.
- Further develop the NCF Framework as a tool for operational analysis. This will include further development of methodologies to assess risks to the NCFs, collecting authoritative sources of data to facilitate assessments, and identifying opportunities to mitigate risk.

These efforts will strengthen the NCF Framework, enhancing the critical infrastructure community's capability to navigate the evolving risk environment and its understanding of critical infrastructure risk to support policymaking and operational decisions. These efforts will also help direct resources to priority security and resilience areas, and aid in early identification of changes in the risk environment. Ultimately, CISA will utilize the NCF Framework with its partners, to stay ahead of threats and protect our way of life.

The NRMCM is grateful to its federal and private sector partners for their support as the functions-based approach matures and develops. CISA will continue to disseminate updates to the functions-based approach as they develop, and always encourages partners to provide NCF-related questions and comments via NCF@hq.dhs.gov. More information on the NCFs is available at [CISA.gov/national-critical-functions](https://www.cisa.gov/national-critical-functions).