



National Critical Functions

Status Update to the Critical Infrastructure Community

July 2020

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



Executive Summary

In the Spring of 2019, the Cybersecurity and Infrastructure Security Agency (CISA), through the National Risk Management Center (NRMC), published a set of 55 National Critical Functions (NCFs) to guide national risk management efforts.

Subsequent to the publication of the NCFs, the NRMC has worked closely with Sector Specific Agencies and private sector representatives of the Critical Infrastructure Partnership Advisory Council to develop a more robust understanding of critical infrastructure risk and risk management.

The NCFs allows for a more robust prioritization of critical infrastructure and a more systematic approach to risk management. The NCFs effectively reset the critical infrastructure risk management framework established in the National Infrastructure Protection Plan. The previous version focused on entity level risk management as opposed to critical outcomes. By establishing a set of critical functions performed by critical infrastructure, the NCF approach enables a richer understanding of how entities come together to produce critical functions, which then contributes to understanding the key assets, systems and networks that contribute to the functions, as well as critical technologies, and dependencies that enable the function.

From the NCF program's inception, it has focused on aggregating information from a diverse set of private and public stakeholders to provide useful analytic products to the widest audience. Integrating characteristics from physical, cyber, social, and regulatory risk analysis is complex and requires analysis of NCFs on an individual basis. It also requires an understanding of the interrelationship of the NCFs. While still relatively new, the NCF framework is being matured and operationalized.

Since the publication of the NCFs, the NRMC has taken several steps, working in concert with the critical infrastructure community, to develop and utilize the NCFs to support risk management. This document describes the outcomes of this effort thus far. The four key lines of effort are:

- Definitions – The NRMC refined the NCF definitions to help guide policy and doctrinal efforts for critical infrastructure security and resilience and cybersecurity
- Planning and Policy Support – The NCFs were used as the basis to support policy making around information and communications technology supply chain risk management, security

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.



of position, navigation and timing systems, and resilience against electromagnetic pulse attacks.

- Operational Support – The NCFs have been utilized to support disaster-specific response and restoration operations. Most prominently, the NCFs have helped prioritize risk management needs for COVID19 response, as well as security need around heightened geopolitical tensions, and preparedness for impending hurricanes.
- Development of the NCF Risk Architecture - Utilizing the National Infrastructure Simulation Analysis Center, the NRMC is developing an enduring risk architecture, supported by risk methodologies and related data sources to enable the critical infrastructure community to have a technology-enabled understanding and visualization of NCF risks.

The NRMC worked closely with the critical infrastructure community to accomplish each of the above.

Since publishing the National Critical Functions, CISA has engaged in substantial conversation with the critical infrastructure community to enhance its understanding of NCF attributes.

The information collected from the critical infrastructure community provided immediately valuable insights and a concrete path forward. It underscores and clarifies the comprehensive interconnections among the Nation’s infrastructure.

As [Politico](#) noted in an article published in May of 2020, the NRMC is “trying to master and define the nation’s critical functions, understand how the U.S. economy actually works and overlay those systems with how they’d be impacted by various events, from cyberattacks to earthquakes.”

The rest of this document highlights NCF progress along the four key lines of effort.

II. Definitions

Working across the critical infrastructure community, the NRMC has defined each of the 55 National Critical Functions. The definitions help scope the risk inherent to each function.

Table 1 National Critical Functions and Definitions

		Function	Definition
Connect	1	Operate Core Network	Maintain and operate communications backbone infrastructure for voice, video, and data transmission that connects to users through broadcasting, cable, satellite, wireless, and wireline access networks
	2	Provide Cable Access Network Services	Provide access to communications backbone infrastructure through fiber and coaxial cable network, supplying analog and digital video programming services, digital telephone service, and high-speed broadband services
	3	Provide Internet Based Content, Information, and Communication Services	Produce and provide technologies, services, and infrastructure that deliver key content, information, and communications capabilities via the Internet



		Function	Definition
Connect	4	Provide Internet Routing, Access, and Connection Services	Provide and operate exchange and routing infrastructure, points of presence, peering points, local access services, and capabilities that enable end users to send and receive information via the Internet
	5	Provide Positioning, Navigation, and Timing Services	Operate and maintain public and private capabilities which enable users to determine location, orientation and time
	6	Provide Radio Broadcast Access Network Services	Operate over-the-air radio and television (TV) stations (operating at medium, very high, and ultra-high frequencies) that offer analog and digital audio and video programming services and data service
	7	Provide Satellite Access Network Services	Provide access to core communications network via a combination of terrestrial antenna stations and platforms orbiting Earth to relay voice, video, or data signals
	8	Provide Wireless Access Network Services	Provide access to core communications network via electromagnetic wave-based technologies, including cellular phones, wireless hot spots (Wi-Fi), personal communication services, high-frequency radio, unlicensed wireless, and other commercial and private radio services
	9	Provide Wireline Access Network Services	Operate circuit- and packet-switched networks via copper, fiber, and coaxial transport media, including private enterprise data and telephony networks and the public switched telephone network (PSTN)
Distribute	10	Distribute Electricity	Maintain and operate medium- to low-voltage system to reliably supply consumer demand for electricity from the bulk electric power network
	11	Maintain Supply Chains	Manage and sustain the networks of assets, systems, and relationships that enable the movement of goods and services from producers to consumers
	12	Transmit Electricity	Maintain and operate high-voltage (>100kV) bulk electric system to reliably supply distribution network demand for electricity from generation resources
	13	Transport Cargo and Passengers by Air	Provide and operate aviation systems, assets, and facilities to enable a system of securely and safely conveying goods and people from place to place by air
	14	Transport Cargo and Passengers by Rail	Provide and operate freight and passenger railroad systems, including conveyances, infrastructure, and management systems to enable a system of securely and safely conveying goods and people from place to place by rail
	15	Transport Cargo and Passengers by Road	Provide and operate roadway systems, assets, and facilities—including commercial motor carriers and associated facilities, motor coaches, buses, and associated systems, assets, and facilities—to enable a system of securely and safely conveying goods and people from place to place by highway



		Function	Definition
Distribute	16	Transport Cargo and Passengers by Vessel	Provide and operate maritime systems, assets, and facilities to enable a system of securely and safely conveying goods and people from place to place by the Maritime Transportation System
	17	Transport Materials by Pipeline	Provide and operate systems, assets, and facilities to enable a system of securely and safely conveying materials from place to place by pipelines
	18	Transport Passengers by Mass Transit	Provide and operate systems, assets, and facilities to enable a system of securely and safely conveying people from place to place by roads or on fixed guideways within a specified geographic area—including transit buses, trolleybuses, monorails, heavy rail (subway), light rail, passenger rail, commuter rail, and vanpool/rideshare
Manage	19	Conduct Elections	Conduct elections, including managing voter registration and rolls, voting infrastructure, polling places, vote counting, and certifying and publishing election results
	20	Develop and Maintain Public Works and Services	Design, build, and maintain infrastructure to supply government services, including systems and assets used for transportation and traffic management, water supply, waste management, recreation, and other purposes
	21	Educate and Train	Provide education and workforce training including PreK-12, community college, university, and graduate education, technical schools, apprenticeships, non-formal education, and on-the-job training
	22	Enforce Law	Operate Federal, State, local, tribal, territorial, and private sector assets, networks, and systems that contribute to enforcing laws, conducting criminal investigations, collecting evidence, apprehending suspects, operating the judicial system, and ensuring custody and rehabilitation of offenders
	23	Maintain Access to Medical Records	Maintain, use, and share actionable data (including personally-identifiable information and personal health information such as care history) effectively, appropriately, bi-directionally and in a timely fashion, for patient care, billing, and operational and clinical research
	24	Manage Hazardous Materials	Safely identify, monitor, handle, store, transport, use, and dispose of hazardous materials (including chemical, biological, radioactive, nuclear, and explosive substances) under normal operations and in response to emergencies
	25	Manage Wastewater	Collect and treat industrial and residential wastewater to meet applicable public health and environmental standards prior to discharge into a receiving body
	26	Operate Government	Carry out legislative, judicial, and executive government missions, including activities related to developing and enforcing codes, ordinances, rules, regulations, and laws; collecting taxes and revenues; managing records, budgets, and finances; and providing public services



	Function	Definition
Manage	27 Perform Cyber Incident Management Capabilities	Provide security systems and services that protect critical business assets and functions, including preventive guidance, simulation, testing, and warning capabilities; operate operations response centers and teams; integrate and share information; coordinate and provide response, recovery, and reconstitution services
	28 Prepare for and Manage Emergencies	Organize and manage resources and responsibilities for dealing with all aspects of emergencies (prevent, protect, mitigate, respond, and recover), to be resilient to and reduce the harmful effects of all hazards
	29 Preserve Constitutional Rights	Secure the principles of freedom and independence and maintain the structures of American government through the protection of rights and processes prescribed in the U.S. Constitution
	30 Protect Sensitive Information	Safeguard and ensure the integrity of information whose mishandling, spillage, corruption, or loss would harm its owner, compromise national security, or impair competitive or economic advantage
	31 Provide and Maintain Infrastructure	Design, construct, operate, repair, survey and improve private and public infrastructure
	32 Provide Capital Markets and Investment Activities	Issue and trade securities, including debt securities (such as bonds), equities (such as stocks), and derivatives (such as options and futures); provide advisory services and related services, such as prime brokerage; maintain operate organized markets and over-the-counter mechanisms for these instruments
	33 Provide Consumer and Commercial Banking Services	Accept and maintain deposit accounts (e.g., checking and savings accounts) and close substitutes (e.g., short-term retail notes) from non-financial intermediaries
	34 Provide Funding and Liquidity Services	Provide funding to non-financial counterparties, such as corporate or retail customers, including individual consumers
	35 Provide Identity Management and Associated Trust Support Services	Produce and provide technologies, services, and infrastructure to ensure the identity of, authenticate, and authorize entities and ensure confidentiality, integrity, and availability of devices, services, data, and transactions
	36 Provide Insurance Services	Operate systems and markets to transfer financial risks among parties through contractual relationships, including products for individuals, corporations, and public-sector entities
37 Provide Medical Care	Ensure the provision of healthcare services	
38 Provide Payment, Clearing, and Settlement Services	Carry out processes required for the exchange of assets, including payment (transfer of funds between or among participants), clearing (transmitting, reconciling, and confirming transactions prior to settlement), and settlement (transfer of ownership and payments)	



		Function	Definition
Manage	39	Provide Public Safety	Provide public services– to include police, fire, and emergency medical services – to ensure the safety and security of communities, businesses and populations
	40	Provide Wholesale Funding	Maintain processes for lending and borrowing among financial services sector parties
	41	Store Fuel and Maintain Reserves	Store energetic materials (including fossil and nuclear fuels) to reliably meet operational and strategic demands
	42	Support Community Health	Conduct epidemiologic surveillance, environmental health, migrant and shelter operations, food establishment inspections, and other community-based public health activities
Supply	43	Exploration and Extraction of Fuels	Identify resources and collect energetic materials (including fossil fuels, nuclear materials, and others)
	44	Fuel Refining and Processing Fuels	Transform raw energetic materials into consumer fuels (e.g., crude cracking, gas separation, and uranium enrichment)
	45	Generate Electricity	Produce electricity from a variety of primary energy sources (including fossil fuels, nuclear materials, and renewables) to reliably meet demand
	46	Manufacture Equipment	Fabricate and assemble components to produce tangible property
	47	Produce and Provide Agricultural Products and Services	Grow and harvest plant and animal commodities (including crops, livestock, dairy, aquaculture, and timber) and produce inputs required to support agricultural production (such as fertilizers, pesticides, animal food, crop seeds, and veterinary services)
	48	Produce and Provide Human and Animal Food Products and Services	Produce food products from raw agricultural commodities and provide to final consumers (including processing, packaging and production, product storage as well as retail and food service)
	49	Produce Chemicals	Manufacture basic chemicals from raw organic and inorganic materials and manufacture intermediate and final products from basic chemicals
	50	Provide Metals and Materials	Manufacture iron, steel, and ferro-alloy products; alumina and aluminum products; non-ferrous metals; and other materials as primary components for other industries
	51	Provide Housing	Construct and/or provide safe and secure permanent or temporary shelter for people (includes physical construction and emergency sheltering)
	52	Provide Information Technology Products and Services	Design, develop, and distribute hardware and software products and services (including security and support services) necessary to maintain or reconstitute networks and associated services
	53	Provide Materiel and Operational Support to Defense	Develop, produce, and sustain defense systems and components and provide support to defense operations



		Function	Definition
Supply	54	Research and Development	Conduct basic research, innovate, test, and introduce new products and services or improve existing products and services
	55	Supply Water	Maintain availability of water (raw and treated)

III. Planning and Policy Support

In April of 2019, National Critical Functions were referenced for the first time in Executive Order via the President’s executive action in Executive Order 13865, “Executive Order on Coordinating National Resilience to Electromagnetic Pulse.” Subsequent to that, additional executive action has been supported by NCF analysis. Highlights of three relevant executive actions are below:

- **Executive Order on Coordinating National Resilience to Electromagnetic Pulses (EMPs)** - The policy of the United States is to prepare for the effects of EMPs through targeted approaches that coordinate whole-of-government activities and encourage private-sector engagement. To support that work, the Secretary of Homeland Security is, in coordination with the heads of relevant SSAs, using the results of risk assessments to better understand and enhance resilience to the effects of EMPs across all critical infrastructure sectors, including coordinating the identification of national critical functions and the prioritization of associated critical infrastructure at greatest risk to the effects of EMPs.
- **Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing (PNT) Services** – To strengthen national resilience, the federal government must foster the responsible use of PNT services by critical infrastructure owners and operators. It is the policy of the United States to ensure that disruption or manipulation of PNT services does not undermine the reliable and efficient functioning of its critical infrastructure. PNT is an NCF and DHS is strengthening it via the processes outlined in the NCF risk framework.
- **Executive Order on Securing the Information and Communications Technology and Services Supply Chain** - To support the national emergency declared by the President, the Secretary of Homeland Security directed the NRMCM to assess and identify entities, hardware, software, and services that present vulnerabilities in the United States and that pose the greatest potential consequences to national security via the NCF framework. The NRMCM completed that analysis in the Fall of 2019 and a description is available here: https://www.cisa.gov/sites/default/files/publications/eo-response-methodology-for-assessing-ict_v2_508.pdf

These activities demonstrate the interaction between the NCF risk framework and policymaking, and the beginning of a common understanding of critical infrastructure risk across hazards. The NCFs, originally mandated through the 2018 National Cyber Security Strategy, have become the lens by which critical infrastructure is evaluated in terms of Information and Communications Technology supply chains, the threat of EMP attacks and similar effects from geomagnetic disturbances, and as a process for ensuring functionality of Global Positioning System and supporting infrastructure.

IV: Operational Support

The NCF structure helped the U.S. Government organize and optimize risk mitigation activities related to homeland security operations. Most prominently, the NCFs have served as a basis for understanding risk to the Nation’s critical infrastructure related to the COVID-19 outbreak. To do so, the NRMCM identified COVID-related drivers that could degrade or disrupt NCFs. To support operations,



the NRMCM assesses the level of impact to the NCFs from these drivers of concern over a 60-day window based on available, reliable information. Analysis focuses on key risk indicators, as well as general monitoring.

- **Driver 1 – Core Commodity Supply Shortage.** A limited supply of a core commodity is available– or something necessary to produce the core commodity – that is essential for the continued reliable operation of the critical function. Example: A national shortage of Personal Protective Equipment affects the ability of the Provide Medical Care NCF to operate reliably.
- **Driver 2 – Shortage of Workers.** A shortage of workers necessary for the continued operation of a critical function exists, either in whole or a crucial subset. This degradation can occur because of illnesses, social distancing policies, diminished transportation systems, or lack of child care. *Worker absenteeism due to illness, quarantining and lack of child care affects the Manufacture Equipment NCF as some assembly lines cannot operate if not completely staffed.*
- **Driver 3 – Significantly Increased Demand for the Critical Function.** A demand increase significantly beyond normal operating parameters which could stress the normal operation of the critical function. *Example: A significant increase in demand for healthcare services affects the reliable operation of the Provide Medical Care NCF.*
- **Driver 4 – Decrease in Demand.** A significant decline in demand for its operation or outputs from COVID-19 impact affects the function. The consequence of a decrease in demand for the function could result from a variety of reasons, including a decline in public confidence in utilizing a critical function or from restrictions placed on use. *Example: A significant decrease in demand affects the normal operation of Transport Passengers by Mass Transit NCF as less demand leads to significant reduction in the transportation service offered.*
- **Driver 5 – Change in cyber posture.** The critical function is experiencing increased use of information and communications technology, new digital platforms, cyber augmentations to business activity, expanded remote access, and/or cascading demand for reciprocal technology-enabled solutions and/or may impacted by cyber-attacks. *Example: Tele-medicine replacing in-person doctor visits, requiring technology enablement among patients, doctors, records or financial systems with new demands on network configuration and data privacy.*

Such driver identification and assessment are critical to how the NCF framework can support operational decision-making. For COVID-19, the NRMCM used the NCF structure to create a register of risks to critical infrastructure from the pandemic. This will serve as a template for broader efforts by the NRMCM to work via stakeholder engagement mechanisms, including the Critical Infrastructure Partnership Advisory Council (CIPAC) structure, to create an NCF risk register.

Going forward the NRMCM is developing other drivers of concern, linked to potential risk scenarios such as cyber-attacks and natural disasters to support protection, response, and restoration activities in operational environments. Layering that with an understanding of how the function works and the level of geographic concentration enables better risk management support.

Geographic Characterization of NCFs

Although all NCFs are national in nature, some of the functions are centrally generated, others are locally generated, and others are hybrid. Risk management strategies for NCFs should be tailored depending on the structure of the NCF.

The NRMCM has characterized the geographic concentration of different NCFs in order to distinguish NCFs that are truly national in scale with potential for national-scale impacts, or a need for national-



scale mitigation measures from those that are more local or regional in nature. Accordingly, a single concentration was assigned to each NCF.

Table 2 Geographic concentrations used to classify NCFs

Concentration	Definition
Local (diffuse)	NCFs that are locally generated, provided or managed where the impacts of disruption would largely be confined to a local area and where interventions would need to be implemented locally
Regional (hotspots)	NCFs for which one or more local or regional concentrations of activity are critical to the performance of the function at the national scale
National (centralized)	NCFs that are nationally created, provided or managed with no geographic concentration
Hybrid (Contingent)	NCFs that are comprised of multiple subsystems that span multiple scales and thus, the geographic concentration is contingent on the specific element of the function of interest

Assignments were made based on the following criteria:

- The geographic distribution of the physical assets and the workforce that support a function. For example, assets that are ubiquitously distributed across the U.S. landscape can be distinguished from those that are concentrated in specific locations or regions.
- The interdependency among geographically disparate assets and workers. For example, geographically dispersed, local functions that are governed and operate independently of one another can be distinguished from regional concentrations of functions that serve the entire nation, or are governed through a centralized authority.

Of the 55 NCFs, almost 20% were recognized as being truly national in nature. 18%, were identified as having regional concentrations. However, a larger percentage (36%) were identified as being distinctly local in nature, implying the function is managed locally and any disruption to the function does not necessarily scale to larger geographic areas. Given the level of aggregation for some of the functions, 27% of the NCFs could not be conveniently classified into a local, regional, or national concentration and are described as hybrids.

V. Risk Architecture Development

The final major line of effort over the last year was the conceptual development of the NCF Risk Architecture. The NCF Risk Architecture leverages a scalable and extensible framework that combines dependencies within (intra-) and between (inter-) NCFs, various data structures, and analytic capabilities to provide decision support through complex cyber and physical critical infrastructure risk analysis.

Preliminary NCF analysis found evidence that the NCF set represents a nested, hierarchical, and bi-directional network. Individual NCFs represent key nodes in the network and future analysis is needed to identify their dependencies.

The risk architecture begins with a decomposition of functions into sub-functions, because each function is a series of process steps supported by key entities. A generic NCF decomposition includes the following.

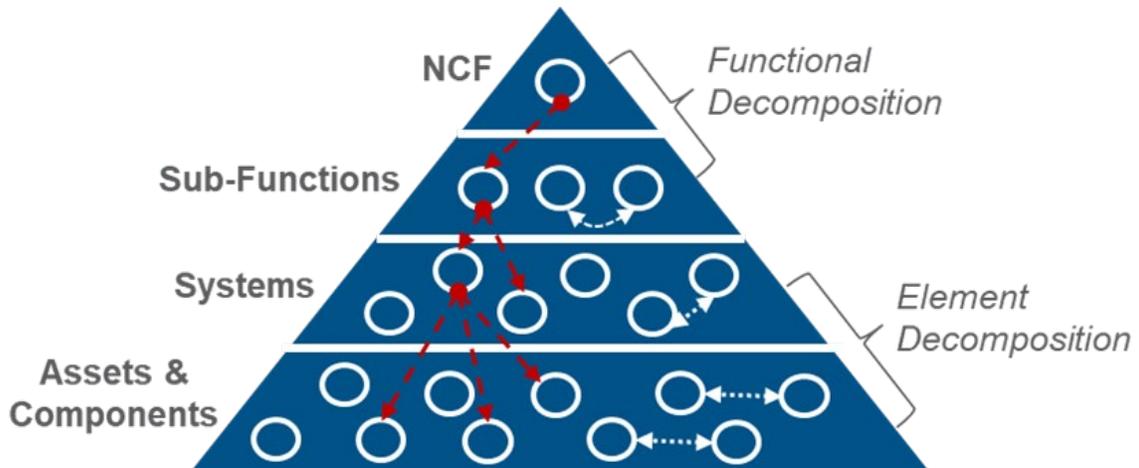


Figure 1 NCF Decomposition

The provision of each NCF involves a complicated series of process composed of sub-processes and dependencies. The NCF risk architecture will build out that understanding. In doing so, it is possible to learn the key assets, networks and systems that support those processes, as well as the underlying software, hardware, and other technologies that enable that process. It is also possible to identify the entities – whether businesses or government – that are key providers of elements of the process and function. The risk architecture relies on process and engineering maps, as well as understanding of business and governance of the function to enable risk analysis against a range of scenarios.

Figure 2 illustrates a decomposition of the Conduct Elections NCF, mapping voter registration steps, through Website reporting of results.

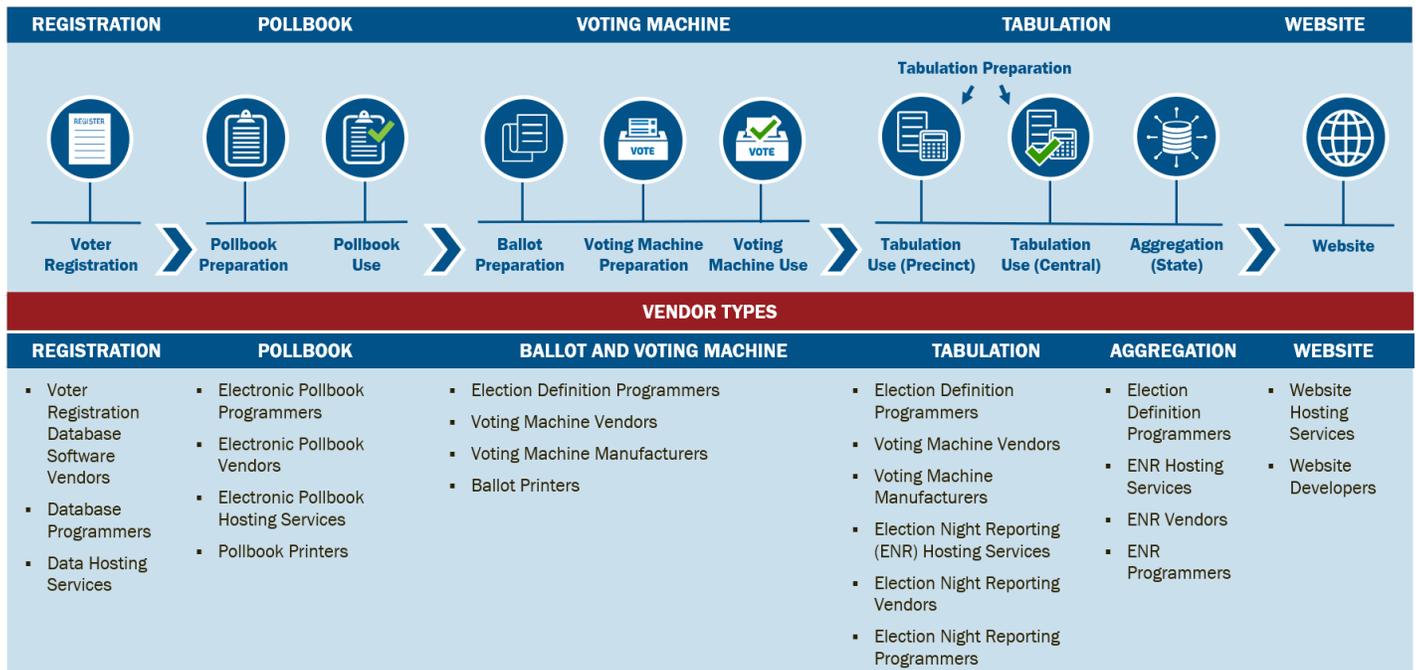


Figure 2 Conduct Elections Decomposition



Ultimately, the risk architecture will decompose all 55 NCFs along these lines:

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 to NCF to NCF dependencies using the NCF definitions
5. Analyze the directionality of NCF to NCF interdependencies

The NRMC will then use the Modeling Capability Transition Environment (MCTE) that CISA is developing to create an interoperable platform where data and models are stored to support decision support analysis. MCTE will also enable data visualization to support planning and operations. Table 3 lays out *potential* decision support visualizations that will be enabled by the NCF risk architecture.

Table 3 Potential Decision-Support Visualizations

Potential Decision-Support Visualizations	
NCF Risk Dashboard	Risk Mitigation Curves
Critical Node Analysis	Geospatial Visualizations
Critical Path Analysis	Supply Chain Spatial Statistics
Nodal Cluster Analysis	Value of Information Analysis
Parameter Sensitivity	Comparative Risk Curves
Tabular Asset Prioritization	And more ...



Conclusion: National Critical Functions: Enabling a Deeper Understanding of Critical Infrastructure Risk

In April 2019, CISA fundamentally shifted how critical infrastructure risk is articulated. The NCFs provide a framework that better portrays the functions that maintain the nation's economy and way of life. This evolved functional perspective enables more comprehensive risk management that considers physical and digital risks; eases challenges identifying and managing risks across industries and stakeholder groups; and provides an organizing structure equally effective in addressing near-term and long-term threats.

This process involved elicitation sessions to identify functions that sectors rely on, provide, or support. Sector stakeholders considered how they would prioritize NCFs based on a series of risk attributes, including the degree to which they rely on each NCF, how severely they would be disrupted by the loss of a function, and their current capability to manage such a disruption.

The data and the insights they provided are the foundation for shaping future NCF efforts. Using the collected information, the NRMC will leverage criteria to prioritize areas for future risk management activities. The criteria focus on the delivery of services; deepening the understanding of stakeholder communities; coordination with the intelligence community; and in-depth research into the activities, capabilities, inter-relationships, and roles and responsibilities that enable the operation of individual NCFs.

This work will continue to help the Nation advance its understanding of critical infrastructure risk to support policy making and operational decisions. It will enable advancements in security and resilience by supporting prioritization decisions for security resource allocations and early identification of broad strategic risk shifts.

CISA will continue to utilize this framework, in concert with our partners, to ensure critical infrastructure risks are identified and reduced.

The NRMC will work to characterize NCF's that that have influence across traditional critical infrastructure sectors, particularly those that are not anchored to any one Sector-Specific Agency.

The NRMC 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 encourage partners to provide NCF-related questions and comments via NCF@hq.dhs.gov. More information on the National Critical Functions is available on our website at www.cisa.gov/national-critical-functions.