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

NATIONAL RISK MANAGEMENT CENTER

OVERVIEW

The **National Risk Management Center (NRMC)** is the planning, analysis, and collaboration center within the In this rapidly evolving threat environment, sources of strategic risk are widespread and include cyber and physical attacks; supply chain vulnerabilities; malicious exploits of emerging technology; nation-state aggression; insider threat; pandemics and natural disasters; and the convergence of previously siloed risks. The NRMC is working with public and private stakeholders to identify, analyze, prioritize, and manage these risks to help advance the Nation's collective defense.

RISK ANALYSIS AND RISK MANAGEMENT PARTNERSHIP

The NRMC's two primary bodies are the Analysis Division and the Planning and Coordination Division.

The **NRMC's Analysis Division** performs risk assessments, modeling, and data management and visualization to understand cross-cutting critical infrastructure risks to support ensuing policy making, process enhancements, and risk management decisions. This division houses the **National Infrastructure Simulation and Analysis Center (NISAC)**, a consortium of National Laboratories and other performers that builds critical infrastructure analytic capabilities.

The **NRMC's Planning and Coordinating Division** actively engages with public and private partners to better understand critical infrastructure operations, identify gaps, develop and execute risk reduction strategies and strengthen critical infrastructure security and resilience. This division oversees risk management initiatives for some of the Agency's top priorities as identified in CISA's Strategic Intent: www.cisa.gov/publication/strategic-intent.

The full range of NRMC's capabilities are leveraged to turn planning and analysis into collective action.

LEVERAGING THE NATIONAL CRITICAL FUNCTIONS FRAMEWORK

Guiding the NRMC's work is understanding risk to National Critical Functions (NCFs)—the functions of government and the private sector so vital to the U.S. 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.

Technological advances and the connectedness of infrastructure systems have resulted in a risk landscape where degradation of assets and impacts from adversarial exploits may have cascading impacts within and across the 16 critical infrastructure sectors and other stakeholder groups. The NCFs are an evolved risk management framework designed to enable rapid response to shifts in the risk environment. By understanding where key dependencies and interdependencies lie between systems, the NRMC works with partners to build resilience to NCFs in a more targeted, prioritized, and strategic manner.

To support this analysis, the NRMC is utilizing NISAC and sector expertise to build an NCF Risk Architecture—a scalable approach supported by risk methodologies and a wide range of critical infrastructure data points to provide CISA and its partners with a technology-enabled understanding and visualization of risks from a range of hazards.

DEFEND TODAY, SECURE TOMORROW

The NRMC's priority risk management initiatives are described below. Each of these efforts rely on effective collaboration and innovation across government and private industry. They include:

5G
Securing the next generation of wireless technology which transforms U.S. telecommunication networks and empowers critical services.

Election Security
Working with a wide of stakeholders and State and local governments to ensure America's election infrastructure is resilient as we #Protect2020 and beyond.

Electromagnetic Pulse and Geomagnetic Disturbance
Mitigating potential nuclear and space weather events that can affect large areas of our nation.

Enterprise Cyber Risk Management
Advancing the emerging discipline of cyber risk quantification by adding analytic rigor to the ability to connect vulnerability management with consequence metrics, and use this information to drive business and national security decisions.

Information and Communications Technology (ICT) Supply Chain Risk Management
Reducing risk of vulnerabilities in the ICT supply chain that if exploited, can impact a wide range of enterprises and sectors dependent on those hardware, software, or services.

Pipeline Cybersecurity
Partnering with front-line operators to assess and manage risk to the design and configuration of control systems for the Nation's 2.7 million miles of pipelines.

Positioning, Navigation, and Timing
Understanding cross-sector reliance on positioning, navigation, and timing services and how we can increase the security and resilience of its delivery.

NRMC RESOURCES

To learn more about the NRMC, visit: www.cisa.gov/national-risk-management.
For questions or to seek additional help, contact us at NRMC@hq.dhs.gov.