# National Risk Management Center

**THE NATIONAL RISK MANAGEMENT CENTER (NRMC) IS HOUSED WITHIN THE DEPARTMENT OF HOMELAND SECURITY'S CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). THE NRMC IS A PLANNING, ANALYSIS, AND COLLABORATION CENTER WORKING TO IDENTIFY AND ADDRESS THE MOST SIGNIFICANT RISKS TO OUR NATION'S CRITICAL INFRASTRUCTURE.**

The NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to: **Identify; Analyze; Prioritize; and Manage** the most strategic risks to our National Critical Functions — the functions so vital that an attack or interruption to services within the government and the private sector could have devastating consequences to our national security, economic security, national public health and safety, or any combination thereof.

## What We Do

Since being announced at the DHS National Cybersecurity Summit, the NRMC has hit the ground running. Specifically:

- **Protecting National Critical Functions:** the NRMC has launched a far-reaching effort across all 16 critical infrastructure sectors to identify and validate a list of National Critical Functions. This allows DHS to assess critical infrastructure interdependencies and identify risk and the impact it would have on our critical functions.
- **Information and Communication Technologies (ICT) Supply Chain Risk Management Task Force:** sponsored by the NRMC, the Task Force is public-private partnership to act as the federal focal point to examine and develop consensus recommendations to identify and manage risk to the global ICT supply chain.
- **Tri-Sector Executive Working Group Risk Management Activities:** chartered with senior industry representatives from the Financial Services Sector, Communications Sector, and Electricity Sub-Sector and senior government representatives from the Departments of Homeland Security, Treasury, and Energy. Efforts have been launched to help direct intelligence collection requirements, build cross-sector risk management playbooks, and better understand systemic risk.
- **Pipeline Cybersecurity Initiative:** leveraging Sector Specific Agency expertise of TSA, and technical cybersecurity capabilities of the NCCIC, this initiative will work with pipeline asset owners and operators to include an in-depth review and evaluation of the control system's network design, configuration, and interdependencies.
- **Election Security and Resilience:** working with state and local election officials, law enforcement, and the Intelligence Community, DHS has led a committed federal effort to increase information sharing with state and local partners, provide technical assistance and vulnerability assessments, strengthen communication channels, and build trust.

The NRMC is also the home within DHS for risk management initiatives surrounding Electromagnetic Pulse, Position, Navigation and Timing, and securing Unmanned Aircraft Systems.

## Managing Risk

The adversaries looking to disrupt our critical infrastructure are no longer shooting from the hip to see what sticks. They are increasingly strategic and deliberate in their efforts to exploit potential Achilles Heels that could cause maximum degradation to National Critical Functions.

Our response needs to be equally strategic and prioritized. It also must recognize that risk resides at a functional level that cuts across assets, organizations, and sectors. This reality is reinforced by the cross-sector importance of supply chain risk management and technologies like Position, Navigation, and Timing.

Over the past decade, strong progress has been made to mature our mechanisms for public-private information sharing, and promote steady engagement through the National Infrastructure Protection Plan Framework and 16 sector structure. This is a solid foundation that must act as a springboard for even deeper partnership.

**The NRMC looks to turn this engagement and awareness into collective action.**

By understanding what is truly critical, where key dependencies and interdependencies lie, and the potential cascading impact of threats, we can identify pockets of risk we deem to be unacceptable for the nation.

Protecting National Critical Functions is a key component of the recently released National Cyber Strategy, and featured prominently in the Joint National Priorities developed in partnership with the critical infrastructure community.

## Defending Today, Securing Tomorrow

The NRMC focuses on the long game of cybersecurity and infrastructure protection. In this capacity, it works with 24/7 operations centers like CISA's National Cybersecurity and Communications Integration Center (NCCIC) and the National Infrastructure Coordinating Center (NICC). By providing a strategic, long-term outlook to complement the daily "blocking and tackling" already taking place, the NRMC is filling a critical risk management gap. With existing operations centers focused on our mission to defend today, the NRMC is focused primarily on securing tomorrow.