Homeland Security

DHS NATIONAL RISK MANAGEMENT CENTER

The threat environment is increasingly complex and interconnected. In response to corresponding demand from industry for enhanced risk management integration with the U.S. Federal government, the Department of Homeland Security (DHS) is refocusing its analysis and planning capabilities. The National Risk Management Center provides a home for collaborative, sector-specific and cross-sector risk management efforts to better protect critical infrastructure.

SUMMARY OF THE NATIONAL RISK MANAGEMENT CENTER

- The National Risk Management Center evolved out of the former Office of Cyber and Infrastructure Analysis. Its cross-cutting risk management approach between the private sector and government will help improve the defense of our nation's critical infrastructure.
- Housed within DHS, the Center enhances NPPD's organizational approach by:
    - Identifying, assessing, and prioritizing strategic risks to national critical functions;
    - Collaborating on the development of strategies and approaches to manage risks to critical functions; and
    - Coordinating integrated cross-sector risk management activities.
- The National Risk Management Center's will provide a single point of access where government and the private sector can collaborate across sectors to develop plans and solutions for reducing cyber and other systemic risks to national and economic security.

PATH FORWARD

The Center will lead a series of activities that will help define what is truly critical; create the frameworks by which government and industry collectively manage risk; and initiate specific cross-sector activities to address known threats.

MORE ABOUT THE MISSION AREAS

Identify, assess, and prioritize risks to national critical functions

GAP: Critical infrastructure protection efforts often have focused on assets and organizations while missing some of the underlying services and functions. As a result, these efforts can underestimate the importance of sector-wide and cross-sector risks and dependencies.

Example: A cross-sector approach that focuses on interdependencies and services can better illuminate the risk calculus of assets like position, navigation, and timing (PNT) infrastructure or industrial control systems.

Immediate Action: Identify national critical functions through risk registries and dependency analyses, with a focus on lifeline functions.

Collaborate on the development of risk management strategies and approaches to manage risks to national critical functions

Gap: Historically, collaboration has focused on information sharing. However, by jointly developing a collaborative risk management strategy through a public-private partnership, it is possible to enable protective efforts to secure critical infrastructure more effective.

Example: Cyber supply-chain efforts have historically focused on eliminating the bad options and have not incentivized or created opportunities for the development of alternative trusted options.

Immediate Action: Develop a strategic framework to identify critical cyber supply-chain elements across critical infrastructure sectors, fostering secure and transparent critical infrastructure supply-chain options.

Coordinate integrated cross-sector risk management activities

Gap: There are opportunities for additional risk management coordination across sectors and between government and industry. Given the cross-cutting nature of critical infrastructure technologies like industrial control systems and the Internet of Things, it is important to close his gap.

Example: Nation-state actors attempt to infiltrate critical infrastructure operations across multiple sectors. Efforts to detect and disrupt, including deploying incident response teams across the country, require operational coordination across government.

Immediate Action: Establish a cross-sector, government/industry playbook for executing integrated risk management activities.