Homeland Security

DHS NATIONAL RISK MANAGEMENT CENTER

IN RESPONSE TO THE INCREASINGLY COMPLEX THREAT ENVIRONMENT AND CORRESPONDING DEMAND FROM INDUSTRY FOR GREATER INTEGRATED SUPPORT FROM THE U.S. FEDERAL GOVERNMENT, THE DEPARTMENT OF HOMELAND SECURITY (DHS) IS ESTABLISHING A JOINT CENTER TO PROVIDE A CENTRALIZED HOME FOR COLLABORATIVE, SECTOR-SPECIFIC AND CROSS-SECTOR RISK MANAGEMENT EFFORTS TO BETTER PROTECT CRITICAL INFRASTRUCTURE.

SUMMARY OF THE RISK MANAGEMENT INITIATIVE

- The National Risk Management Center will create a cross-cutting risk management approach between the private sector and government to improve the defense of our nation's critical infrastructure.
- The Center, housed within DHS, establishes an organizational approach to integrate risk management activities, perform joint strategic planning, and most importantly, develop collaborative solutions to reduce risk to critical infrastructure.
- The National Risk Management Center will:
  - ✓ identify, assess, and prioritize efforts to reduce risks to national critical functions, which enable national and economic security;
  - ✓ collaborate on the development of risk management strategies and approaches to manage risks to national functions; and
  - ✓ coordinate integrated cross-sector risk management activities.
- The National Risk Management Center's mission is to provide a simple and single point of access to the full range of government activities to mitigate a range of risks, including cybersecurity, across sectors.

PATH FORWARD

The Center will be a government and industry partnership to coordinate risk management efforts, initially by leading 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.

NATIONAL RISK MANAGEMENT MISSIONS

- ✓ Identify, assess, and prioritize risks to national critical functions
- ✓ Collaborate on the development of risk management strategies and approaches to manage risks to national critical functions
- ✓ Coordinate integrated cross-sector risk management activities

MORE ABOUT THE MISSION AREAS

Identify, assess, and prioritize risks to national critical functions

Gap: Critical infrastructure protection efforts have too often been focused on assets and organizations while missing some of the underlying services and functions, which can underestimate the importance of sector-wide and cross-sector risks and dependencies.

Example: Some critical national functions may fall outside of traditional infrastructure categorization, so 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 and industrial control systems.

Immediate Action: The Center will 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: Focus of collaboration to date has been on information sharing, which is essential. In addition, however, a collaborative risk management strategy that is jointly developed through a public-private partnership would elevate the effectiveness of protective efforts to secure critical infrastructure.

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: Risk management activities are frequently stove-piped and opportunities exist for additional coordination across sectors and between government and industry, a distinct need given the cross-cutting nature of critical infrastructure technologies like industrial control systems and the Internet of Things.

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. Lessons learned include the need for an agreed-upon playbook to integrate government and industry response efforts.

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