Homeland Security

Joint National Priorities for Critical Infrastructure Security and Resilience

CALLED FOR IN THE NATIONAL INFRASTRUCTURE PROTECTION PLAN (NIPP), THE JOINT NATIONAL PRIORITIES FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE BUILD UPON AN EVALUATION OF EMERGING RISKS, KNOWN CAPABILITY GAPS, RESOURCE AVAILABILITY, AND BEST PRACTICES. THE 2018 JOINT NATIONAL PRIORITIES ARE INTENDED TO FOCUS THE CRITICAL INFRASTRUCTURE COMMUNITY'S EFFORTS IN ADVANCING THE SECURITY AND RESILIENCE OF THE NATION'S CRITICAL INFRASTRUCTURE. THE PRIORITIES HELP PROVIDE SUPPORT TO CRITICAL INFRASTRUCTURE SECTORS IN DRAFTING THEIR SECTOR PLANS AND HELP INFORM DECISION-MAKING FOR CRITICAL INFRASTRUCTURE STAKEHOLDERS. THE CRITICAL INFRASTRUCTURE COMMUNITY HAS MADE GREAT STRIDES IN ADVANCING THE FIRST SET OF PRIORITIES ISSUED IN OCTOBER 2014. THESE UPDATED PRIORITIES EMPHASIZE THE IMPORTANCE OF BUILDING ON THOSE ADVANCES TO CONTINUE IMPROVING THE SECURITY AND RESILIENCE OF THE NATION'S CRITICAL INFRASTRUCTURE IN THE FACE OF A COMPLEX RISK ENVIRONMENT.

STRENGTHENING RISK MANAGEMENT AND PRIORITIZATION OF CYBER AND PHYSICAL THREATS AND HAZARDS IS A NATIONAL PRIORITY. THESE PRIORITIES ARE CONSISTENT WITH THE NATIONAL SECURITY STRATEGY.

Reduce Risk to National Critical Functions

Critical infrastructure is increasingly interconnected, creating new challenges to critical infrastructure operations and system-wide functionality. Moving toward systems-level thinking in risk management decision making is a critical step in understanding and mitigating the risks that are created by evolving physical and cyber threats. Working with industry, the government will track, understand, prioritize, and communicate risks to critical infrastructure through a functional, systems-based approach. Utilizing a prioritized risk management structure, the government will be better positioned to prioritize threats and vulnerabilities, and ensure appropriate focus depending on the tactical, operational, or strategic nature of the problem set. This systems-level risk evaluation and prioritization should also be applied to improving security of soft targets, crowded places, public venues, and special events.

To improve the utilization of a systems-based approach, the critical infrastructure community should identify national critical functions to better understand systemic risks that involve impacts that propagate in interconnected systems. These risks could include those created by prevalent equipment, software, and IT services, as well as associated supply chains. They can also involve insiders. To achieve system-wide risk management, the critical infrastructure community should explore policy, technological, behavioral, and organizational solutions that can be used to improve security and resilience across operating environments and ensure critical functions can be maintained.

Enhance Incident Response and Recovery Capabilities

Critical infrastructure restoration is a life sustaining imperative. The critical infrastructure community should support the rapid restoration of lifeline functions by using an integrated, cross-sector approach that is built into response and recovery doctrine to share resources, expertise, and timely and relevant information during and following incidents. Coordination is critical during catastrophic events in order to determine priorities and align resources for optimal impact on supporting communities and saving lives. Government and industry should collaborate during incident response and infrastructure restoration, ensuring the best available business and infrastructure data is available to support response and recovery priorities.

As part of this collaboration, the critical infrastructure community should leverage and expand existing national and international partnerships by incorporating partnership efforts and capabilities into operational plans. Partnership efforts should incorporate a unified assessment of when increased operational coordination might be required and if that coordination should be within the private sector or between the Government and the private sector. Partnership plans should also articulate mutual priorities, identify and address changes in the threat environment, and lay out objectives for restoration, prioritization, and recovery. Partnership structures should include definitions of what available actions, authorities, information flows, processes, and resources can be used to achieve objectives.

Improve Information Sharing

Sharing timely, relevant information and intelligence promotes awareness of threats, hazards, and national security concerns relating to critical infrastructure. Information sharing enables risk mitigation measures and improves understanding of threats, interdependencies, and collective preparedness efforts. It can also help reduce exposure to developing threats, minimize the duration and impact of incidents, and accelerate the return to normal operations in the aftermath of physical or cyber incidents.

The critical infrastructure community should promote an information sharing culture and strengthen government and private sector frameworks. Using the functional, systems-based approach to risk management, the government can strengthen existing frameworks to inform community-wide analytical priorities and guide planning efforts. The critical infrastructure community should continue to develop new mechanisms for rapid and reliable information sharing, to include enhancements at the state, local, and regional level and the ability to better contextualize threats. The critical infrastructure community should also evaluate how it can improve its information sharing efforts by using emerging technologies. Emerging technology, such as automated data collection and analytics, can facilitate information dissemination, more precise characterization of threats, and the development of new information sharing channels. The critical infrastructure community should also strive to break down barriers to effective information sharing.

Protect Critical Infrastructure Against Nation-state Cyber Threats

Our adversaries are increasingly looking to critical infrastructure as a potential target space for geopolitical aims via cyber attacks. The critical infrastructure community should clearly address nation-state cyber threats in cybersecurity strategies and plans as part of an overall national security effort. Where possible, these efforts should include identifying and reducing potential cyber threat vectors and developing strategies for improving operational resilience. The critical infrastructure community should continue to develop and implement programs, practices, methodologies, and resources that address these changing threats, with a particular focus on safeguarding critical infrastructure from potential cyber threats driven by hostile nation-states. This approach should also include addressing insider and counter intelligence threats as well as risks associated with foreign investment.

The critical infrastructure community should work to advance the collective cyber defense model to address systemic and catastrophic cyber risks. This model should include a focus on collaboration, information sharing, and identification of methods for leveraging entities' respective capabilities. This will also necessitate more integration of national security and economic security analysis to ensure that Nation-states are not introducing undue risk into cyber systems through foreign investment.

Homeland Security

Drive Security and Resilience in Investment and Innovation

The critical infrastructure community has broadly started adopting security and resilience into infrastructure design, planning, and decision-making. The critical next step is to expand these early adopters' efforts into larger-scale plans, industry standards and best practices, and subsequent infrastructure development and operation. The critical infrastructure community should support increased public and private investments in secure and resilient critical infrastructure.

The critical infrastructure community should continue to improve its investment processes by expanding its understanding of the factors that can drive the use of security and resilience concerns in critical infrastructure decision-making. Understanding the incentives that currently drive investment in critical infrastructure will make it possible to guide, inform, prioritize, and leverage across the community, actions that promote more secure and resilient infrastructure. That support should also identify and explore new financing mechanisms that can support investments in the development and deployment of measures that enhance security and resilience against all hazards. Finally, it is important to address innovation in security and resilience by design and invest in additional research and development to aid these efforts.