The 2014 Quadrennial Homeland Security Review

Overview:

Four years ago, the Department of Homeland Security's first quadrennial review answered the question, "What is homeland security?", laying out the vision, five mission areas, and goals and objectives for homeland security.

This second quadrennial review reflects a more focused, collaborative Departmental strategy, planning, and analytic capability. The risk-informed priorities set forth in this Review will drive operational planning, as well as analysis of resource and capability options and tradeoffs over the next four years. The Review also recognizes the responsibility the Department shares with hundreds of thousands of people across the federal, state, local, tribal, and territorial governments, the private sector, and other nongovernmental organizations, and provides a path forward for engaging in public-private partnerships. These are the people who regularly interact with the public, who are responsible for public safety and security, who own and operate our nation's critical infrastructure and services, who perform research and develop technology, and who keep watch, prepare for, and respond to emerging threats and disasters.

To access a copy of the 2014 QHSR, please visit www.dhs.gov/QHSR.

Safeguard and Secure Cyberspace

Each and every day, the United States faces a myriad of threats in cyberspace, from the theft of U.S. intellectual property through cyber intrusions to denial-of-service attacks against public facing websites and attempted intrusions of U.S. critical infrastructure. The Department of Homeland Security (DHS) works closely with government and private sector partners to strengthen cybersecurity capabilities, investigate cybercrime, and share actionable information to ensure a secure and resilient cyberspace that protects privacy and other civil liberties by design, supports innovation and economic growth, and helps maintain national security, and public health and safety.

Of growing concern is the cyber threat to critical infrastructure. The essential services that we all rely on—including energy, telecommunications, water, transportation, and financial services—are increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide-scale or high-consequence events which could harm or disrupt the American way of life and economy.

Strategic Priorities

Strengthen the Security and Resilience of Critical Infrastructure

We must draw on the Nation's full range of expertise and resources—from all levels of government, the private sector, members of the public, and international partners—to secure critical infrastructure from cyber threats. Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (2013), and Presidential Policy Directive 21 "Critical Infrastructure Security and Resilience" (2013) establish a risk-informed approach and a framework for critical infrastructure security and resilience. This collective approach to prevent, protect against, mitigate, respond to, investigate, and recover from cyber incidents prioritizes understanding and meeting the needs of our partners.

Secure the Federal Civilian Government Information Technology Enterprise

The Federal Government must serve as a model to other organizations by securing our networks with the latest tools, information, and capabilities. Our approach will help federal civilian agencies manage cyber networks through strategically sourced tools and services that enhance the speed and cost-effectiveness of federal cybersecurity procurements and allow consistent application of best practices.

Advance Law Enforcement, Incident Response, and Reporting Capabilities

Through close coordination, law enforcement entities, cybersecurity experts, state, local, tribal, and territorial partners, critical infrastructure owners and operators, and private sector partners will increase the quantity and effectiveness of cybercrime investigations and network security efforts to identify and respond to malicious actors, and will continue to grow our nation's cyber incident response and information-sharing capabilities.

Strengthen the Ecosystem

Cybersecurity is a shared responsibility in which everyone has a role to play. Ensuring a healthy cyber ecosystem will require collaborative communities domestically and abroad, innovative security solutions, standardized and consistent processes to share information and best practices, and development of a skilled workforce to ensure those policies and plans are implemented effectively.