



Strategy for Quadrennial Homeland Security Review (QHSR) Mission 4 – Safeguarding and Securing Cyberspace Terms of Reference

February 2011

I. Overview

Cyber infrastructure forms the backbone of the Nation’s economy and connects every aspect of our way of life. While the cyber environment offers the potential for rapid technological advancement and economic growth, a range of malicious actors may seek to exploit cyberspace for dangerous or harmful purposes, disrupt communications or other services, and attack the Nation’s infrastructure through cyber means. By statute and Presidential directive, DHS has the lead for the Federal government to secure civilian government computer systems, to work with industry to defend privately-owned and operated critical infrastructure, and to work with State, local, tribal and territorial governments to secure their information systems. This mission, to Safeguard and Secure Cyberspace, is one of five homeland security missions established by the 2010 Quadrennial Homeland Security Review (QHSR).

The 2010 QHSR was the first step in establishing the strategic path forward to guide the activities of the homeland security enterprise toward a common end: a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive. Consistent with and expanding upon the President’s National Security Strategy, the QHSR accomplished this vision by establishing key mission priorities and specific goals and objectives for each of those mission areas. Ultimately, these goals and objectives form a framework, at the grand strategy level, of basic end-states that we must realize in order to succeed in the missions.

The QHSR also articulates three core concepts:

- Security: Protect the United States and its people, vital interests and way of life;
- Resilience: Foster individual, community, and system robustness, adaptability, and capacity for rapid recovery; and
- Customs and Exchange: Expedite and enforce lawful trade, travel, and immigration.

All homeland security activities, including Mission 4: Safeguarding and Securing Cyberspace, must be built upon a foundation of ensuring security and resilience, as well as facilitating the normal, daily activities of society and interchange with the world.

The next critical step in clarifying and refining homeland security strategic guidance is to identify the specific ways and means by which the QHSR end-states will be realized. These “mission strategies” will provide a subordinate layer of specificity and detail in order to give

tangible and meaningful direction to those that must carry out these missions at an operational level each day across the homeland security enterprise.

To initiate this next level of strategy, the DHS National Protection & Programs Directorate and the DHS Office of Policy will partner to develop a mission strategy for QHSR Mission 4, Safeguarding and Securing Cyberspace. This is the first of five mission strategies that DHS will develop in close partnership with stakeholders across the homeland security enterprise.

II. QHSR Vision Statement

Our vision is a cyberspace that supports a secure and resilient infrastructure, that enables innovation and prosperity, and that protects privacy and other civil liberties by design. It is one in which we can use cyberspace with confidence to advance our economic interests and maintain national security under all conditions.

III. Scope

The 2010 QHSR established the concept of the homeland security enterprise, which refers to the collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners—as well as individuals, families, and communities—to maintain critical homeland security capabilities. Maturing and strengthening the homeland security enterprise includes enhancing shared awareness of risks and threats, building capable communities, fostering unity of effort, and fostering innovative approaches and solutions through leading-edge science and technology.

Homeland security will only be optimized when we fully leverage the distributed and decentralized nature of the entire enterprise in the pursuit of our common goals. While the Department of Homeland Security is charged with homeland security, DHS is only one component within the larger enterprise, and success in this mission space requires the shared commitment of all stakeholders. The importance of strong coordination and collaboration is further emphasized in Presidential policy guidance, including the President’s Cyberspace Policy Review.

To that end, the scope of the strategy is the scope of Mission 4 of the QHSR: safeguarding and securing U.S. government civilian networks and private sector networks. The strategy for Safeguarding and Securing Cyberspace will adopt a homeland security enterprise perspective, and will set forth specific ways and means by which the enterprise will achieve desired national end-states for cybersecurity, respecting current statutory roles and responsibilities. The strategy will complement other strategies for the defense of U.S. government military and classified networks and other cybersecurity activities undertaken by the U.S. government that do not fall under the leadership responsibilities of DHS.

Within the context of an enterprise approach, the strategy will address the homeland security aspects of cybersecurity, as defined by the Secretary of Homeland Security’s authorities set forth in the Homeland Security Act of 2002; the USA PATRIOT Act of 2001; the DHS

Appropriations Act for FY07; 18 U.S.C. § 3056; 18 U.S.C. 2252 and 2252A; the Federal Information Security Management Act of 2002; Homeland Security Presidential Directive 23/Cybersecurity Policy; and the May 2009 Cyberspace Policy Review, among other guiding authorities and/or policies. The strategy will be coordinated with the ongoing review of cybersecurity roles, responsibilities, authorities, and policies by the National Security Staff's Cybersecurity Directorate.

IV. Current Strategy and Policy

The strategy for Safeguarding and Securing Cyberspace will be informed by and build upon current cyber security strategy and policy as outlined in several key documents: Homeland Security Presidential Directive (HSPD) 7, HSPD 23/NSPD 54; the 2003 National Strategy to Secure Cyberspace; the Comprehensive National Cybersecurity Initiative (the CNCI); and the 2009 White House 60-Day Cyberspace Policy Review.

V. Strategic Foundation—QHSR

The strategy for Safeguarding and Securing Cyberspace will build upon the following goals and objectives from the 2010 QHSR:

Goal 1: Create a Safe, Secure, and Resilient Cyber Environment. Ensure malicious actors are unable to effectively exploit cyberspace, impair its safe and secure use, or attack the Nation's digital infrastructure.

Understand and prioritize cyber threats. Identify and evaluate the most dangerous threats to Federal civilian and private-sector networks and the Nation.

Manage risks in cyberspace. Protect and make resilient information systems, networks, and personal and sensitive data.

Prevent cyber crime and other malicious uses of cyberspace. Disrupt the criminal organizations and other malicious actors engaged in high-consequence or wide-scale cyber crime.

Develop a robust public-private cyber incident response capability. Manage cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action.

Goal 2: Promote Cybersecurity Knowledge and Innovation. Ensure that the nation is prepared for the cyber threats and challenges of tomorrow.

Enhance public awareness. Ensure that the public recognizes cybersecurity challenges and is empowered to address them.

Foster a dynamic workforce. Develop the national knowledge base and human capital capabilities to enable success against current and future threats.

Invest in innovative technologies, techniques, and procedures. Create and enhance

science, technology, governance mechanisms, and other elements necessary to sustain a safe, secure, and resilient cyber environment.

VI. Strategy Development Process Guidelines

The strategy for Safeguarding and Securing Cyberspace will:

- Begin from the security environment and key concepts set forth in the QHSR Report.
- Serve as the governing strategic guidance for Mission 4 until it is reviewed as part of the Fiscal Year 2014 QHSR process
- Set forth measurable ways and means for achieving core end states
- Reflect input from a broad range of stakeholders
- Inform the FY13-17 Future Years Homeland Security Program (FYSHSP) and the FY13 Budget.
- Evaluate whether existing authorities are adequate to achieve the desired end states for the strategy.

VII. Process

Strategy development and analysis will proceed in three distinct phases to ensure adequate and appropriate consideration of all critical aspects of strategy development and analysis, namely:

- **Strategy Input**
 - Clarify the Scope and Leadership Intent
 - Review Relevant Literature
 - Understand the Environment
 - Describe Strategic Assumptions
 - State the Overall Vision
 - Determine Core Decision Criteria
- **Strategy Development**
 - Set First-Order Goals
 - Generate and Develop Strategic Concepts
 - Assess Selected Strategy Against Core Decision Criteria
- **Decision**
 - Prepare Selected Strategy for Presentation
 - Convene Relevant Decision Fora

VIII. Structure

The strategy will be developed by representatives from across DHS pursuant to a strategy methodology developed by the Office of Policy. Within DHS, an action officer-level core team

will meet periodically to conduct analysis and frame issues for consideration by a senior-level management group, which will provide critical direction and guidance throughout the process.

In line with the enterprise-level scope of the strategy, the strategy process will include extensive outreach to the homeland security enterprise. At key points throughout the development of the strategy, there will be briefings as well as electronic communication with key enterprise stakeholders in the critical infrastructure sector, with State and local governments, with Federal agencies, with the Congress and other partners including organizations focused on privacy as well as civil rights and civil liberties. This will allow consideration and inclusion of stakeholder inputs into the strategy. Outreach to other Federal agencies will be accomplished through an interagency working group.

IX. Implementation and Next Steps

Once completed, approved and signed by the Secretary, the strategy will be promulgated across the Department and homeland security enterprise. It will also serve as the baseline for requirements analysis and capabilities development efforts across the enterprise.

The final Mission 4 strategy as well as outputs during its development will inform the FY 2013-17 FYHSP, the FY13 budget, and future budgets.