THE ASPEN INSTITUTE
HOMELAND
SECURITY
GROUP

Cybersecurity & the Department of Homeland Security

Recommendations of the Aspen Homeland Security Group's Cyber Working Group for the Department of Homeland Security

The Aspen Institute Homeland Security Group's Cyber Working Group

10/11/2012

THE ASPEN INSTITUTE
HOMELAND
SECURITY
GROUP

Editors

Daniel Prieto
Vice President and Practice Lead
Public Sector Strategy & Innovation
IBM Global Business Services

Evan Wolff
Partner & Director
Homeland Security Practice
Hunton & Williams LLP

Contributors

Charles Allen
Principal
The Chertoff Group

Stewart Baker
Partner
Steptoe & Johnson, LLP

Michael Chertoff
Chairman & Co-Founder
The Chertoff Group

Richard Clarke
Managing Partner
Good Harbor Consulting

Michael Hayden
Principal
The Chertoff Group

Jim Lewis
Director & Senior Fellow
Technology and Public Policy Program
Center for Strategic & International Studies

Guy C. Swan III
Vice President
Association of the United States Army

Starnes E. Walker III
Chief Technology Officer & Technical Director
U.S. Fleet Cyber Command/U.S. 10th Fleet

John Watters
Chairman & CEO
iSIGHT Partners, Inc.

Juan Zarate
Senior Adviser
Transnational Threats Project and Homeland Security and Counterterrorism Program
Center for Strategic and International Studies

Philip Zelikow
Associate Dean
Graduate School of Arts & Sciences
University of Virginia

Aspen Homeland Security Group Staff

Evan Wolff
Deputy Director

Clark K. Ervin
Executive Director

Leah Dreyfuss
Associate

Introduction

At the request of Homeland Security Secretary Janet Napolitano (the Secretary), the Aspen Cyber Working Group seeks to make recommendations to help prioritize and focus the Department of Homeland Security's (DHS's or the Department's) cyber activities.

Cybersecurity, which includes data protection, information security and industrial control systems, represents a national security concern. As discussed below, DHS has significant authority to lead and coordinate, along with other civil agencies, the nation's defensive capabilities including all civil cybersecurity and private sector issues. The Department of Defense (DoD) is responsible for our nation's offensive cybersecurity capabilities, including cyber warfare. Under this framework, the following paper discusses the challenges and considerations that the Aspen Cyber Working Group believes are deserving of the Department's attention.

DHS Cybersecurity Authorities and Mission

The cybersecurity mission and authorities of the Department of Homeland Security are established in federal statute, Presidential Directives and Departmental policies and guidance.[i] Based on these authorities and guidance, DHS has two broad roles.

DHS's first role is to undertake activities focused on national cybersecurity issues and to engage private sector owners and operators of the nation's critical infrastructure and key resources (CIKR) on these issues.[ii] To accomplish these responsibilities, DHS engages in the collection, protection and dissemination of critical infrastructure information, including cyber threat information, (HSA, Section 201) and provides technical assistance upon request to critical infrastructure owners and operators (HSA, Section 223). These DHS responsibilities are further reinforced by HSPD-7 which has roles for both physical and cyber security and requires DHS to "serve as a focal point for the security of cyberspace . . ." with a mission that includes "analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems." Pursuant to HSPD-7, DHS is also responsible for developing the National Infrastructure Protection Plan, a plan that outlines national goals, objectives, milestones, and key initiatives necessary for fulfilling the Department's responsibilities for physical and cyber critical infrastructure protection across all 18 critical infrastructure sectors.

DHS's second significant role is to serve as the lead federal agency responsible for coordinating critical infrastructure protection efforts in nine specific sectors: Non-military/non-intelligence Government Facilities; Chemicals; Commercial Facilities; Critical Manufacturing; Dams;

Emergency Services; Information Technology; Nuclear Reactors; Materials and Waste; Postal and Shipping; Telecommunication; and Transportation. DHS's role in Chemical sector security is further defined by the Chemical Facility Anti-Terrorism Standards (CFATS), which gives DHS lead authority to regulate security, including cybersecurity, at high-risk chemical facilities.[iii]

Each of these DHS cybersecurity roles has been reinforced by the Comprehensive National Cybersecurity Initiative (CNCI), established by President Bush pursuant to HSPD-23/NSPD-54.[iv] The CNCI identifies twelve activities focused on national cybersecurity issues and clarifies the relevant DHS roles and responsibilities including managing Trusted Internet Connections, deploying intrusion detection and prevention systems across the Federal enterprise, and coordinating a broad range of Federal cybersecurity strategies. Also, CNCI calls for the definition of the Federal role in extending cybersecurity into critical infrastructure. Although CNCI has galvanized much of the DHS and other federal cybersecurity programs, many of its activities and details remain classified. Additionally, Executive Order 13603, 77 Fed. Reg. 16,651 (March 22, 2012), delegates to the Secretary of each federal department and agency the authority "to take actions necessary to ensure the availability of adequate resources and production capability, including services and critical technology, for national defense requirements."[v] DHS has additional responsibility regarding the civilian Federal networks, including responsibilities under the Federal Information Security Management Act (FISMA).

DHS also led the interagency office in publishing the Quadrennial Homeland Security Review (QHSR) which developed a multi-step process for securing the homeland and outlined missions and priorities intended to achieve that goal. Among those stated missions are to "create a safe, secure, and resilient cyber environment" and to "promote cybersecurity knowledge and innovation."[vi] In its "Blueprint for a Secure Cyber Future" (Blueprint) DHS proposes a path for achieving the goals it developed in the QHSR.[vii] Specifically, the Blueprint describes two areas of action: protecting our nation's critical information infrastructure today and building a stronger cyber ecosystem for the future.

As DHS recognized in the QHSR, the Department's homeland security missions are "enterprise-wide and not limited to the Department of Homeland Security."[viii] Federal cybersecurity leadership for other sectors rests outside of DHS. For example, the DoD is responsible for cybersecurity for Defense systems and assets as well as those possessed by the Defense Industrial base (DIB); the Department of the Treasury maintains authorities for cybersecurity in the financial and banking sector; the Department of Energy is responsible for energy sector cybersecurity; the Environmental Protection Agency for water; Health and Human Services for health; the Department of Agriculture and the Food and Drug Administration for agriculture and food, and the Department of the Interior for national monuments and icons.[ix] These lead federal agencies, referred to as sector-specific agencies (SSAs), are responsible for coordinating critical infrastructure protection efforts with the public and private stakeholders in their respective sectors and for providing input to the NIPP.

DHS Cyber Activities and Organization

Given the broad nature of DHS's national cyber mandate and the relative narrowness of areas where Congress directs that mandate, DHS has significant discretion regarding how it pursues a wide range of strategic, tactical, and operational activities in order to achieve its legally-established cyber mission. As a general matter, DHS cyber activities include education, coordination, seeking to influence behavior through incentives or regulation, operational activities including analysis and incident response, and research and development (R&D). Specific activities DHS has undertaken pursuant to its mandate include:

- DHS established the Office of Infrastructure Protection (OIP) which included the National Cyber Security Division (NCSD) and addressed both physical and cybersecurity issues. NCSD was later split off into a separate division of the Office of Cybersecurity and Communication (CS&C) in order to ensure that cyber issues received their own separate and prioritized focus. Both OIP and CS&C currently reside in the National Protection and Programs Directorate (NPPD). OIP focuses primarily on physical infrastructure and is organized around infrastructure sectors. CS&C focuses on cybersecurity and is organized and structured around watch functions (*i.e.,* United States Computer Emergency Readiness Team (US-CERT)/Industrial Control Systems Emergency Response Team (ICS-CERT)/National Cybersecurity and Communications Integration Center (NCCIC)) and mission functions (*i.e.,* federal civilian networks and providing technical assistance to the private sector).

- DHS developed the NIPP. While the current NIPP has a large physical security focus, cybersecurity is included and can be adapted to include additional activities.

- In support of the NIPP, DHS established associated frameworks to manage a public private partnership. This was formalized under the Critical Infrastructure Partnership Advisory Council (CIPAC) and consists of a set of Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) for each sector. For many of the sectors, DHS has facilitated the establishment of Information Sharing and Analysis Centers (ISACs).

- DHS has developed various watch and emergency watch centers, including the National Infrastructure Coordinating Center (NICC), National Cybersecurity and Communications Integration Center (NCCIC), US-CERT, and ICS-CERT.

- DHS conducted outreach activities regarding physical and cyber infrastructure protection activities both nationally (*i.e.*, G-First and CIPAC meetings) and regionally (*i.e.*, Protection Security Advisor (PSA) Program).

- DHS created the regulatory CFATS program which includes physical security and cybersecurity requirements for high risk chemical facilities.

Proposals to Enhance DHS

Various legislative and Executive proposals under consideration by Congress and the Administration over the past few years seek to clarify and/or augment DHS cyber authorities and activities. These proposals include clarifying and/or augmenting existing authorities that would:

- Increase DHS authority to issue and enforce regulations requiring private sector critical infrastructure (CI) owners to strengthen cybersecurity;

- Revise FISMA, giving DHS increased authority over federal Information Technology (IT) systems, especially as regards continuous monitoring and compliance enforcement;

- Enhance DHS capability for incident reporting; and

- Provide enhanced personnel authorities related to cyber personnel.

Recommendations

In light of DHS's existing authorities and regardless of potential new legislation, we believe that DHS has an opportunity now to rationalize and refocus its cybersecurity efforts. Many DHS capabilities are unclear or are still being developed. DHS too often does not present a unified face to partners who seek its assistance. Fragmentation in DHS cyber activities makes it difficult for other federal agencies and private sector players to know when it is appropriate to turn to DHS for help, and what capabilities DHS possesses to provide assistance. DHS should take steps to clarify its capabilities, value proposition and operating models to other federal players and to the private sector as regards cyber preparedness, response, and recovery.

DHS can and should make choices regarding the role it plays relative to the market and relative to other government stakeholders, the private sector and the public. The roles that DHS selects for itself, and the interaction of those roles on a program-by-program basis, will determine the cost and resource intensiveness of its cyber efforts. By building capabilities and focusing efforts in areas unique to DHS, DHS can improve the efficacy and cost-effectiveness of the programs it pursues.

1) ***FOCUS:*** *DHS should focus its cyber activities in areas of national significance where it possesses a clear mandate and/or where it possesses unique skills, capabilities or competence. Specifically, these areas will include those where:*

   a) *there is a clear capabilities gap that would not otherwise be filled by other governmental entities or by the private sector,*

   b) *the impact of Computer Network Attack/Computer Network Exploitation (CNA/CNE) poses cross-sector, cascading, or systemic risk to CIKR, or*

   c) *there is potential involvement of a national security or foreign actor thereby requiring that DHS coordinate appropriately with DoD, the Intelligence Community, and/or the Federal Bureau of Investigation (FBI).*

   DHS should evaluate the value of its activities in areas that do not meet these criteria and consider whether to maintain such activities.

2) ***STREAMLINE AND SIMPLIFY:*** *DHS should streamline and simplify its cyber-related organizational structure to provide unified command and unity of effort, making it easier for partner agencies and for the private sector to be aware of and understand DHS capabilities and to interact efficiently with DHS.*

3) ***INTEGRATE:*** *DHS should ensure that its civil CIKR cybersecurity and physical activities are fully integrated with its private sector and partner agencies to ensure clarity and avoid confusion and redundancy. In order to accomplish successful integration, DHS should:*

   a) *develop a unified/coordinated outreach plan and a common notification system for providing alerts and warnings to private sector CIKR owners across physical and cybersecurity issues,*

   b) *develop standard operating procedures (SOPs) for interacting with private sector CIKR entities suffering CNA/CNE.*

   DHS's SOPs should address how information voluntarily shared by the private sector in the course of working with DHS on response and recovery will be protected and include liability *protections for private sector entities who share incident information in the course of seeking technical assistance from the Department. Liability protections may include, for example, blanket pre-approvals from DOJ.*

4) ***STRATEGIC OUTREACH:*** *DHS should refine and clarify its unique capabilities, roles and responsibilities from other governmental entities based upon distinct parts of the security lifecycle:*

a) prepare (NPPD),

b) protect (U.S. Secret Service (USSS)/U.S. Customs and Border Protection (CBP)/U.S. Immigration and Customs Enforcement (ICE)/NPPD),

c) respond (USSS/Federal Emergency Management Agency (FEMA/NPPD), and

d) recover (FEMA/NPPD).

To the greatest extent possible, DHS should designate a single, readily-identifiable, point of contact for each of these roles and responsibilities.

5) ***COORDINATE:*** *The White House should issue an executive order establishing a cybersecurity interagency process. This process would allow coordination of cyber missions and goals with appropriate government departments and agencies. As necessary, DHS should develop interagency Memoranda of Understandings (MOUs) with the FBI, DoD, and other Federal SSAs on strategies for responding to CNA/CNE that impact federal civilian agencies and private sector CIKR entities to support advancement of the executive order.*

6) ***ESTABLISH OPERATIONS CENTER:*** *The White House should issue an executive order directing DHS to establish a single operations center for analytic and information sharing operations to consolidate its current numerous and overlapping centers, including US-CERT, NCCIC, and ICS-CERT. Similar to the National Counterterrorism Center (NCTC), a single and unified DHS operations center should*

a) serve as the primary non-military, non-foreign-intelligence national repository for information on cyber threats,

b) include wider interagency and private sector involvement,

c) provide event analysis and trend analysis and forecasting,

d) catalog and integrate information on threats to private sector CIKR and the .gov domain nationwide,

e) *disseminate information regarding security incidents, attributions and trends as well as mitigation measures, and*

f) *provide a dynamic nationwide map of cyber threats and trends.*

7) ***ADVISE:*** *DHS should develop an advisory committee – similar to DoD's Defense Science Board or the Intelligence Community's (IC's) JASON program – to ensure that the Secretary has ready access, through a regular forum, to cybersecurity technical expertise from outside of the federal government. Members of such a committee should possess high-level security clearances that allow them to work on short term studies and analysis to support the Secretary.*

8) ***TRAIN AND CERTIFY:*** *DHS should establish training programs for federal Chief Information Officers (CIOs) and certification programs for executives at Critical Infrastructure Protection (CIP) operators. Such programs would be supported significantly by providing mechanisms for those individuals to receive classified information so that trainees can have unimpeded insight into classified threat information. This would enhance their ability to protect their networks and to understand the functions, roles, and capabilities of the various government agencies that can assist them in real-world conditions.*

9) ***RESEARCH AND DEVELOPMENT:*** *DHS should define and establish a 5-year research agenda focusing on cyber risks to CIKR that pose national-level concern, e.g. cascading or systemic risks. Possible R&D focus areas include CIKR interdependency modeling and modeling that can assess the system-wide benefits of cybersecurity measures taken within individual CIKR sectors.*

[i] The Homeland Security Act of 2002, Pub. L. No.107-296, 116 Stat. 2135 (2002), (the Act or HSA) establishes DHS as the Federal government's lead agency responsible for securing civilian government computer systems and for working with industry and governments to secure critical infrastructure and information systems. Additionally, the Act provides DHS with authority to work with the private sector on a broad set of cybersecurity issues, including the collection, protection and dissemination of critical infrastructure information (Section 201) and to provide technical assistance upon request from critical infrastructure owners and operators (Section 223). Homeland Security Presidential Directive 7 (HSPD-7), signed by President George W. Bush in 2003, further clarified DHS authority by identifying critical infrastructure sectors and, for each sector, designating a federal Sector-Specific Agency (SSA) to lead protection and resilience-building programs and activities. HSPD-7 required DHS to "serve as a focal point for the security of cyberspace . . ." with a mission that included "analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems." As discussed below, later Presidential Directives have reinforced DHS's authorities. *See, e.g.*, Homeland Security Presidential Directive 23 and National Security Presidential Directive 54 (HSPD-23/NSPD-54) which include broad initiatives that focus

primarily on federal activities and securing federal information-sharing systems and define the role of cyber security in private sector domains.

[ii] In establishing a national directive that Federal departments and agencies identify and prioritize the nation's critical infrastructure and key resources and protect them from terrorist attack, HSPD-7 required heads of all Federal agencies to "develop . . . plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate." Within the NIPP framework, DHS has "emphasized the importance of collaboration and partnering with and among the various partners and its reliance on voluntary information sharing between the private sector and DHS." U.S. Gov't Accountability Office, GAO-10-296, "Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience" at 7 (March 2010).

[iii] Section 550 of the DHS Appropriations Act of 2007 (Pub. L. No. 109-295, 120 Stat. 1355 (2006) gave DHS the authority to establish CFATS for facilities that use, store or manufacture high risk chemicals identified in the Act. CFATS requires covered facilities to develop site security plans (SSPs) appropriate to their relative risk. These SSPs must address eighteen Risk-Based Performance Standards (RBPS), including RBPS 8 which requires consideration of nine categories of policies and practices, including performance metrics, to provide security for the facility's cyber systems. Generally, CFATS provides broad authority to DHS to enter, inspect, and audit chemical facility property, equipment, operations and records that DHS determines present high levels of physical and cyber security risk, and it provides DHS with authority to impose civil fines for noncompliance.

[iv] The CNCI established "the policy, strategy, and guidelines to secure federal systems" and delineated "an approach that anticipates future cyber threats and technologies, and requires the federal government to integrate many of its technical and organizational capabilities to better address sophisticated threats and vulnerabilities." At the national level the CNCI focuses on three key areas (1) establishing a frontline defense to reduce current vulnerabilities and prevent intrusions; (2) defending against the full spectrum of threats by using intelligence and strengthening supply chain security; and (3) shaping the future environment by enhancing the nation's research, development and education as well as investing in leap-ahead technologies. In 2009, President Obama ordered a thorough review of federal efforts to defend the nation's information and communications infrastructure and the development of a comprehensive approach to securing its digital infrastructure. In May 2009, the President accepted the recommendations of the resulting Cyberspace Policy Review, including expanding cybersecurity outreach with the private sector using current legislative authorities.

[v] Under the Defense Production Act of 1950, Executive Order 13603 aims to ensure that the United States has an industrial and technological base capable of meeting national defense requirements. Addressing both war and peace time responsibilities, the Order delegates to the Secretary of each federal department and agency the authority to "plan for and issue regulations to prioritize and allocate resources and establish standards and procedures by which the authority shall be used to promote the national defense, under both emergency and non-emergency conditions." *Id.* at 16,652.

[vi] *See* DHS, "Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland," at 4 (Feb. 2010).

[vii] DHS, "Blueprint for a Secure Cyber Future, The Cybersecurity Strategy for the Homeland Security Enterprise" (Nov. 2011).

[viii] "Quadrennial Homeland Security Review Report" at 19.

[ix] U.S. Gov't Accountability Office, GAO-09-969, "Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment" at 27 (Sept. 2009).