The Heritage Foundation

ISSUE BRIEF

No. 4335 | JANUARY 26, 2015

Congress Should Refocus DHS on Crucial Cybersecurity Reforms

David Inserra

Several weeks ago, President Barack Obama announced that the Department of Homeland Security (DHS) would provide work authorization and protection from deportation to as many as 5 million unlawful immigrants. While Heritage has written on the harm done by the President's executive actions to the U.S. immigration system and the rule of law, another serious side effect is the harmful redirection of attention and resources away from pressing homeland security issues ranging from terrorism to emergency preparedness to institutional reform at DHS. In order to implement the President's sweeping order, DHS Secretary Jeh Johnson and other leaders at DHS will simply not have the time, money, manpower, or trust of Congress to make important reforms to these other areas of critical importance. It falls to Congress to correct these misplaced priorities.

One important area where DHS needs to do more is cybersecurity. DHS is directly or indirectly responsible for large segments of federal cybersecurity as well for supporting private-sector cybersecurity measures. With cyber attacks and threats on the rise, Congress should call on DHS to focus more on making the U.S. more secure in cyberspace.

This paper, in its entirety, can be found at **http://report.heritage.org/ib4335**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

Enhancing U.S. Cybersecurity

In the past year, numerous high-profile hacks of private companies, as well as of government agencies, have kept cybersecurity in the public eye. Even more worrying are reports pointing to various sectors of critical infrastructure being penetrated by nation-state hackers.[1] To better defend all users from cyber attacks and cyber espionage, DHS should be dramatically expanding its ability to engage with the private sector and retain a highly skilled workforce. With DHS's focus elsewhere, Congress should push DHS to improve in several areas.

- Congress should do more to enable cyber-threat and cyber-vulnerability information sharing. Allowing the private sector and public sector to more easily share information with each other will benefit both sides.[2] By providing strong liability protection for information that is shared, businesses will be encouraged to share with the government as well as with other businesses. A clear framework should be established to facilitate information sharing. While DHS might be the most appropriate place to base an information-sharing hub, questions about DHS's capabilities together with privacy concerns could make this difficult. The better path would be a public-private partnership organization with representatives from the government, the private sector, and privacy organizations overseeing the sharing of information. DHS would be an important provider and consumer of this information, enhancing cybersecurity across the board.

- Congress should help DHS improve and expand its ability to monitor government networks. The DHS-run "Einstein" intrusion-detection-and-prevention system has grown dramatically over the past decade, with DHS reporting that 80 percent of traffic at civilian government agencies was monitored in fiscal year 2013.[3] With better information sharing, Einstein's ability to detect and prevent intrusions would be enhanced, but the system must always be improved as the nature of the threats change. Congress should prioritize the continued improvement and expansion of the Einstein system.

- Congress should also do more to counter the security threat to our cyber supply chain. While the Einstein system can detect and prevent intrusions, supply chain threats do not penetrate a system through an e-mail or Web traffic but instead bypass such protections since they are installed in the hardware or software of a system. With the huge growth in technology products, the supply chain for computer and technology products has spread across the world, allowing goods to be produced at lowest cost but with increased risk of counterfeit or malicious products. In 2012, a Government Accountability Office (GAO) study found that the Department of Homeland Security had not "defined supply chain security measures" and as a result was "not in a position to have implementing procedures or monitoring capabilities to verify compliance."[4] In response, DHS stated that it agreed with the assessment and would examine the path forward. While DHS certainly needs to improve its own supply-chain security system, Congress can encourage the development of a private cyber-sector supply-chain rating and accreditation system.[5] Using such a system would be voluntary for companies but would provide their products with a certain seal of security, helping private and public actors purchase goods with the appropriate level of supply-chain integrity.

- Congress should more closely oversee DHS cybersecurity efforts at public and private facilities across the United States. The Federal Protective Service (FPS) is responsible for the physical protection of around 9,000 federal facilities. The GAO found in December 2014, however, that DHS did not have a strategy to define and address the problem of cyber vulnerabilities to building and access control systems. Though FPS technically has purview over cybersecurity, it does not have the expertise to protect these systems. Without a strategy to assign roles and responsibilities, no one in DHS is currently assessing or addressing risk to building control systems.[6] Another report by the GAO in June 2014, found that the Coast Guard and FEMA had major failings in their responsibilities to keep ports cyber-secure.[7] A DHS Inspector General report released in July 2014 found that the Domestic Nuclear Detection Office's efforts to protect its systems from mali-

1. Douglas Ernst, "Russian Hackers' 'Trojan Horse' Malware Inside U.S. Critical Infrastructure Since 2011," *The Washington Times*, November 6, 2014, http://www.washingtontimes.com/news/2014/nov/6/russian-hackers-trojan-horse-malware-inside-us-cri (accessed January 22, 2015), and "Operation Cleaver," Cylance, 2014, http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf (accessed January 22, 2015).
2. David Inserra and Paul Rosenzweig, "Cybersecurity Information Sharing: One Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2899, April 1, 2014, http://www.heritage.org/research/reports/2014/04/cybersecurity-information-sharing-one-step-toward-us-security-prosperity-and-freedom-in-cyberspace.
3. U.S. Department of Homeland Security, "Budget-In-Brief FY 2015," 2014, p. 97, http://www.dhs.gov/sites/default/files/publications/FY15BIB.pdf (accessed January 22, 2015).
4. U.S. Government Accountability Office, "IT Supply Chain: National Security-Related Agencies Need to Better Address Risks," GAO–12–361, March 2012, http://www.gao.gov/assets/590/589568.pdf (accessed January 22, 2015).
5. David Inserra and Steven P. Bucci, "Cyber Supply Chain Security: A Crucial Step Toward U.S. Security, Prosperity, and Freedom in Cyberspace," Heritage Foundation *Backgrounder* No. 2880, March 6, 2014, http://www.heritage.org/research/reports/2014/03/cyber-supply-chain-security-a-crucial-step-toward-us-security-prosperity-and-freedom-in-cyberspace#.
6. U.S. Government Accountability Office, "Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems," GAO–15–6, December 2014, http://www.gao.gov/assets/670/667512.pdf (accessed January 22, 2015).
7. U.S. Government Accountability Office, "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity," GAO–14–459, June 2014, http://www.gao.gov/assets/670/663828.pdf (accessed January 22, 2015).

cious insiders and control and update its systems fell short.[8] Congress should carefully oversee DHS's efforts in these areas to ensure that these shortfalls are being corrected.

- Congress and DHS must improve morale of DHS staffers. In the 2014 "The Best Places to Work in the Federal Government" rankings, the National Protection and Programs Directorate (NPPD), which handles most critical infrastructure and cyber-protection duties in DHS, was ranked the eighth-worst agency subcomponent.[9] Coming in at 308 of 315 organizations, morale at the NPPD is incredibly low, which makes it difficult to recruit and keep good employees, especially when private-sector cybersecurity jobs are available. Notably, pay is not the central issue in this survey; the lack of leadership, training, and performance-based rewards are blamed and must be fixed. If DHS is to be an effective actor in defending U.S. cyberspace, more must be done to improve morale and maintain a highly skilled workforce.

Better Priorities for Homeland Security

In defending and justifying the President's executive action on immigration, Secretary Johnson talked about the need to prioritize scarce resources for immigration enforcement. With DHS's leadership now focused on implementing and defending the executive action, it has implicitly prioritized the President's executive action over other important homeland security issues. Congress must refocus DHS's efforts to make the U.S. more cyber-secure.

*—**David Inserra** is a Research Associate for Homeland Security and Cybersecurity in the Douglas and Sarah Allison Center for Foreign and National Security Policy, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation.*

8. U.S. Department of Homeland Security Office of the Inspector General, "Domestic Nuclear Detection Office Has Taken Steps to Address Insider Threat, But Challenges Remain," OIG-14-113, July 2014, http://www.oig.dhs.gov/assets/Mgmt/2014/OIG_14-113_Jul14.pdf (accessed January 22, 2015).
9. Partnership for Public Service, "The Best Places to Work in the Federal Government: National Protection and Programs Directorate (DHS)," 2015, http://bestplacestowork.org/BPTW/rankings/detail/HS20 (accessed January 22, 2015).