Written Statement of

Michelle Richardson, Legislative Counsel

American Civil Liberties Union

Washington Legislative Office

On

"DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure"

Before the

House Homeland Security Committee

March 13, 2013

AMERICAN CIVIL LIBERTIES UNION

WASHINGTON LEGISLATIVE OFFICE

915 15th Street, NW Washington, D.C. 20005

(202) 544-1681 Fax (202) 546-0738

Good morning Chairman McCaul, Ranking Member Thompson, and Members of the Committee. Thank you for the opportunity to testify on behalf of the American Civil Liberties Union (ACLU), its more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide, about the role of the Department of Homeland Security (DHS) in protecting the cybersecurity of critical infrastructure.

The topic of today's hearing is very timely. DHS is currently the lead agency running major cyber programs on behalf of the government and critical infrastructure, but Congress is considering establishing a new information-sharing regime that could collect cyber information notwithstanding any of the privacy laws currently protecting Americans' sensitive and personal data, and some proposals are unfortunately questioning the role of DHS. Most Americans would agree that the enhancement of online security is a worthy and appropriate goal for those vested with the responsibility for safeguarding the interests of all Americans. Protecting the right to internet privacy – a right with roots in our constitutional principles opposing unreasonable search and seizure and assuring limited government - is as critical a goal as enhancing online security, and DHS is the agency best positioned to handle such new authority in an effective and accountable manner. We look forward to working with this Committee to ensure that these new cyber programs remain under civilian, rather than military control, and that Congress conducts extensive oversight of all DHS programs to ensure protection of privacy rights.

Cybersecurity programs can and must be run in accordance with the Constitution and American values.[1] The internet is an incredibly useful and empowering tool that enhances public knowledge, broadens the reach of our free speech rights, and eases and facilitates daily business and personal activities. As a result, internet data is rich in intimate details of our private and professional lives, such as where we go, with whom we associate, what we read, our religious faith, political leanings, financial status, mental and physical health and more. Protecting privacy is necessary for the public to feel confident in continuing to engage with new and developing technology; any cybersecurity initiatives should make protecting that privacy a paramount goal.

[1] The American Civil Liberties Union's letters to Congress, comments to federal agencies, blogs and other cybersecurity materials may be found at http://www.aclu.org/cybersecurity.

Many existing and proposed cyber efforts do not threaten the privacy or civil liberties of every day internet users, and we urge this Congress and the administration to pursue those programs and to avoid alternative proposals that risk creating major new and unnecessary surveillance programs. Appropriate programs for congressional or administrative action include those to secure government and military networks, educate the public on hygiene issues, prosecute internet-based financial crimes, invest in research and development, secure the supply chain of hardware, and share targeted threat information with critical infrastructure.

I. The Importance of Keeping Domestic Cybersecurity Programs within Civilian Agencies

Under longstanding American legal requirements and policy traditions, the military is restricted from targeting Americans on American soil. Instead, domestic intelligence and law enforcement activities are run by civilian authorities. Some are now arguing that cybersecurity should be the exception, and that military agencies like the National Security Agency (NSA) should be empowered to collect more information about every-day American internet users in order to respond to online threats. Doing so would create a significant new threat to Americans' privacy, and must be avoided.

To date, the military vs. civilian debate has been skewed by the intense focus on cybersecurity threats posed by hostile foreign governments, or international terrorists, and the comparative inattention to threats unrelated to national security. While advanced persistent threats from foreign actors are real and require a multifaceted response from the government, it does not follow that all cybersecurity incidents impacting domestic internet users should merit a military response. Even by intelligence community estimates, those dangers represent a small portion of the threats that affect American internet users. Malware, financial crimes and other threats that do not rise to the level of international incidents make up the overwhelming majority of malicious conduct on the internet. The conflation of foreign spying and potential sabotage, with corporate espionage, everyday internet crime, political statements and essentially prank behavior has inflated every internet malfeasance into a potential national disaster. This hyperbole is simply not factually accurate, and only serves to encourage policy decisions with serious privacy and civil liberties implications.[2]

Placing cyber programs under the jurisdiction of domestic civilian agencies like DHS has real and far more positive consequences for transparency and accountability. DHS's lead competition for cyber programs – the NSA-- is a black hole of information. Programs housed there, like in the rest of the intelligence community, are not subject to any meaningful public oversight. The NSA's activities appear to be presumptively classified, and whatever oversight

[2] See, for example, Howard Schmidt, *Price of Inaction Will Be Onerous*, NYT, Oct. 18, 2012, *available at* http://www.nytimes.com/roomfordebate/2012/10/17/should-industry-face-more-cybersecurity-mandates/price-of-inaction-on-cybersecurity-will-be-the-greatest.

that takes place is cabined in the Intelligence Committees, which conduct most of their business behind closed doors.

One only need look to intelligence wiretapping for an example of the dangers posed if Congress hands control over domestic cybersecurity to the NSA. In 1978, Congress established the Foreign Intelligence Surveillance Act (FISA) to govern foreign intelligence electronic surveillance. Federal judges meeting in a secret court issued opinions interpreting Americans' constitutional rights and developed a secret body of law that the American public has not been allowed to read. The extreme secrecy around such intelligence programs helped conceal a program of illegal and warrantless wiretapping for over six years. Congress eventually amended the FISA to permit this warrantless surveillance to continue, but included a sunset provision that was scheduled to expire at the end of last year. Congress reauthorized it without having a single open hearing with administration witnesses to explain how this expansive authority affects Americans' privacy. While some claim this evolution of expanded wiretapping as a success of the intelligence oversight process, it reflects the limits and consequences of housing these programs behind the intelligence wall.[3]

If cybersecurity – with a set of programs dominated by non-military and non-national security concerns - is ceded to the NSA, this Committee, rank and file members of Congress, and the American public will never hear of it again. Keeping cybersecurity within DHS and other civilian agencies, and within the jurisdiction of this Committee would enhance, not harm, both security and privacy.

II. The Current Role of the Department of Homeland Security in Cybersecurity

Developments over the last several years have rightly steered domestic programs into the DHS or other civilian agencies. In 2010, the Secretary of DHS and the director of the National Security Agency (NSA) signed an agreement that put DHS in charge of cybersecurity in the U.S., with the NSA providing support and expertise.[4] The President's recent Executive Order 13636 continues this approach, putting DHS and the National Institute of Standards and Technology atop the domestic cyber hierarchy, with consultation from the Attorney General, the Privacy and Civil Liberties Oversight Board, and the Office of Management and Budget.[5] These major structural and policy commitments add to longstanding DHS programs that share information with companies and infrastructure operators, educate the public, and secure government systems.

---

[3] The Supreme Court recently ruled in Amnesty v. Clapper that ACLU clients lacked standing to challenge the FISA Amendments Act of 2008, because they could not prove that surveillance of their communications under the act was "certainly impending," all but foreclosing meaningful judicial review of that statute's constitutionality..

[4] MEMORANDUM OF AGREEMENT BETWEEN THE DEPARTMENT OF HOMELAND SECURITY AND THE DEPARTMENT OF DEFENSE REGARDING CYBERSECURITY, September 27, 2010, *available at* http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

[5] Executive Order 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739, February 12, 2013 [hereinafter Executive Order].

DHS's role in the collection, use, and dissemination of cybersecurity information has substantially grown over the last several years. With the recent executive order, its participation will expand again, especially in two areas. First, DHS will run the Enhanced Cybersecurity Services program and facilitate the sharing of threat indicators with critical infrastructure owners and operators.[6] Information sharing in this direction – from government to private sector – has far fewer privacy implications than the reverse. It does however cement DHS' role in information sharing and publicly available Privacy Impact Assessments suggest that the agency is imposing meaningful privacy protections for the personally identifiable information (PII) coming into its possession. For example, PII is not maintained in a system of records, and therefore is not searchable by name or other identifiers, and information is not retained unless it is "directly relevant and necessary" to address a cyber threat.[7]

Second, DHS will coordinate a review of current information sharing programs to determine whether they meet the ideas in the Fair Information Practice Principles (FIPPs).[8] Currently, there is little publicly available information about what agencies are currently doing with cybersecurity information and this annual report will be the first overarching review of these programs.

III. Emerging Domestic Information Sharing Programs Must Be Run By Civilian Agencies Such as DHS

Congress is considering a significant expansion of the government's authority to collect cybersecurity information, and if the expansion moves forward, it is critical for civil liberties that they be run by civilian agencies such as DHS. H.R. 624, the Cyber Intelligence and Sharing Protection Act (CISPA), would exempt cybersecurity information sharing from all privacy laws and reverse decades of statutory protections for sensitive information like our communication, financial, and internet information. It would permit corporations to determine what information pertains to cybersecurity and allow them to share it with the government – including military agencies like the NSA - and other corporations without making a reasonable effort to shield or scrub out personally identifiable information that is unnecessary to address the threat at hand. Companies would then be free to use Americans' sensitive private information as they see fit, and the government could use it for certain reasons other than cybersecurity. When one of those reasons – national security – is wholly undefined, we are especially concerned that the military and intelligence agencies accessing that information would consider themselves to have free reign over such private records, under ever expanding arguments of what national security includes. These and other fundamental problems are why the ACLU continues to oppose CISPA.

---

[6] *Id*. at 4(c).

[7] PRIVACY IMPACT ASSESSMENT FOR ENHANCED CYBERSECURITY SERVICES, January 16, 2013, *available at* http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf, at 7.

[8] Executive Order at (5).

One of the biggest problems with CISPA is that it does not require companies that participate in this new information sharing regime to work with civilian agencies, and instead allows them to share sensitive and personal information directly with the NSA and other military agencies. The bill's sponsors claim that American corporations insist on dealing with the NSA and may withhold this information from the government altogether if directed to go elsewhere. This assertion does not stand up, especially considering that the companies in question are not part of the defense sector, and primarily offer services to the public and the private sector. Companies that actually have defense information are already permitted to participate in a NSA-run information regime, and other potentially targeted sectors can continue to work with the agencies that have long regulated them.

CISPA insists on giving the companies the authority to share domestic, civilian internet information directly with the NSA even though it neither wants nor needs it. NSA Director General Keith Alexander has stated that his agency should not be the public face of cybersecurity and does not need to directly receive domestic cyber information.[9] In fact, the House Intelligence bill is an outlier. The administration's Statement of Administration Policy on CISPA in the 112th Congress, said that the bill

> …effectively treats domestic cybersecurity as an intelligence activity and thus, significantly departs from longstanding efforts to treat the Internet and cyberspace as civilian spheres. The Administration believes that a civilian agency – the Department of Homeland Security – must have a central role in domestic cybersecurity, including for conducting and overseeing the exchange of cybersecurity information with the private sector and with sector-specific Federal agencies.[10]

The Senate's most recent information sharing legislation, Title VII of the Cybersecurity Act of 2012, also made clear that cybersecurity information should only go to a civilian

---

[9] Jennifer Martinez, *General: Nation Needs DHS Involved in Cybersecurity*, THE HILL, Oct. 21, 2012, *available at* http://thehill.com/blogs/hillicon-valley/technology/259547-general-nation-needs-dhs-involved-in-cybersecurity-, ("I see DHS as the entry point for working with industry," [General Keith] Alexander said at an event hosted by the Wilson Center and National Public Radio…Alexander stressed that protecting the nation's critical infrastructure requires a team effort from the government, including the involvement of DHS. "Where I sit, it's our job to help them be successful. I think they're taking the right steps and it's the right thing to do," Alexander said. "Our nation needs them to be in the middle of this."); Kim Zetter, *DHS, Not NSA Should Lead Cybersecurity, Pentagon Official Says*, WIRED, Mar. 1, 2012, *available at* http://www.wired.com/threatlevel/2012/03/rsa-security-panel/ ("'Obviously, there are amazing resources at NSA, a lot of magic that goes on there,' said Eric Rosenbach, deputy assistant secretary of Defense for Cyber Policy in the Department of Defense. 'But it's almost certainly not the right approach for the United States of America to have a foreign intelligence focus on domestic networks, doing something that throughout history has been a domestic function.' Rosenbach, who was speaking at the RSA Security conference in San Francisco, was adamant that the DHS, a civilian agency, should take the lead for domestic cybersecurity, with the FBI taking a strong role as the country's domestic law enforcement agency.").

[10] OFFICE OF MANAGEMENT AND BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY, H.R. 3523, CYBER INTELLIGENCE SHARING AND PROTECTION ACT, April 25, 2012, *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/sap/112/saphr3523r_20120425.pdf.

agency.[11] While a handful of amendments to CISPA passed on the House floor last year, none of them addressed this point. Members of the Intelligence and Homeland Security Committees filed amendments that would have required new domestic information sharing to be routed through civilian agencies, but they were not made in order and did not receive a vote.[12] The administration, the Senate, and the privacy community are in agreement that civilian control of these programs is not only good for civil liberties, but workable from a cyber and national security standpoint. CISPA stands alone in failing to follow this common wisdom.

IV. Further Areas for Committee Oversight of DHS Cybersecurity

Because of the House's imminent efforts to expand information sharing and the importance of keeping those programs in civilian hands, this statement has focused on that proposal and how it fails from a civil liberties and privacy perspective. But we also urge this Committee to undertake oversight activities of existing cybersecurity programs. In particular, we urge the Committee to review the implementation of the EINSTEIN program, which works with providers to scan government systems for known cyber threats. The last Privacy Impact Assessment on EINSTEIN was written in 2010 and there is little public information about the broader application of the program and the effectiveness of privacy requirements. The Committee should also make sure that agencies are participating meaningfully in the FIPPs review discussed above so that DHS can do an overarching analysis of whether privacy is protected in current programs.

V. Conclusion

Thank you for the opportunity to share our views on cybersecurity and the role of DHS. The administration is giving DHS increasing responsibilities in this area and we hope that if information collection programs expand, they too are housed in DHS. We look forward to working with you on this and other civil liberties issues in the future.

[11] S. 3414, The Cybersecurity Act of 2012, 112th Cong. (2012).

[12] CISPA amendments filed with the with the House Rules Committee are available at http://rules.house.gov/Legislation/legislationDetails.aspx?NewsID=812. Amendment 19 by House Permanent Select Committee on Intelligence member Representative Jan Schakowsky (D-IL) and amendment 21 by House Homeland Security Committee Ranking Member Bennie Thompson (D-MS) would have ensured that new sharing under CISPA would have gone to civilian agencies and DHS respectively.