COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, U.S. DEPARTMENT OF COMMERCE

"Request for Information: Developing a Framework To Improve Critical Infrastructure Cybersecurity"

April 8, 2013

By notice published on February 26, 2013, the National Institute of Standards and Technology ("NIST") of the Department of Commerce requested information "to help identify, refine, and guide the many interrelated considerations, challenges, and efforts needed to develop" a framework to reduce cyber risks to critical infrastructure.[1] Under Executive Order ("EO") 13636, NIST is tasked with developing a framework for reducing cyber risks to critical infrastructure (the "Cybersecurity Framework" or "Framework").[2] Accordingly, "[t]he Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[3] Importantly, the Cybersecurity Framework requires "methodologies . . . to protect individual privacy and civil liberties."[4]

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus on emerging civil liberties issues and protecting privacy, the First Amendment, and constitutional values. EPIC has a long history of promoting transparency and accountability for cybersecurity

---

[1] Developing a Framework to Improve Critical Infrastructure Cybersecurity,78 Fed. Reg. 13,024 (Feb. 26, 2013) [hereinafter "Request for Information"].
[2] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).
[3] *Id.* at 11,740-41.
[4] *Id.* at 11,741.

and government data collection programs, specifically through the enforcement of the Privacy Act and the Freedom of Information Act.[5] Transparent cybersecurity programs are crucial to the public's ability to monitor the government's efforts and ensure that federal agencies respect privacy rights and comply with their obligations under the Privacy Act. EPIC further supports techniques that improve both privacy and security.

EPIC supports basing privacy and civil liberty protections on the Fair Information Practices.[6] Additionally, EPIC supports the review of the Department of Homeland Security's ("DHS") activities by the Chief Privacy Officer and the Officer for Civil Rights and Civil Liberties. EPIC also supports the Executive Order's call for a public report that evaluates agency activities against the Fair Information Practices ("FIPs").[7] In addition, EPIC agrees that the Framework "should include flexible, extensible, scalable, and technology-independent standards, guidelines, and best practices."[8] As the Department of Commerce explores a broad framework for cybersecurity, EPIC recommends addressing a number of fundamental concerns and consider the following additional recommendations to improve the Cybersecurity Framework.

Within the scope of the Cybersecurity Framework, EPIC recommends that NIST: (1) with respect to any cybersecurity legislation, urge Congress to include protections for civil liberties and privacy in line with the Cybersecurity Framework; (2) abide by the

[5] *See EPIC v. NSA*, 678 F.3d 926 (D.C. Cir. 2012); EPIC, Cybersecurity Privacy Practical Implications, http://epic.org/privacy/cybersecurity/; EPIC, *EPIC v. NSA – Cybersecurity Authority*, http://epic.org/privacy/nsa/epic_v_nsa.html; EPIC, Comments of the Elec. Privacy Info. Ctr. to the Cyber Security and Information Assurance Research and Development Senior Steering Group of the Federal Networking and Information Technology Research and Development Program: Request for Comments, Dec. 19, 2012, *available at* http://epic.org/privacy/cybersecurity/EPIC-DOD-Cyber-Security-Comments.pdf.

[6] *Id.* at 11,740 ("Such [privacy and civil liberty] protections shall be based upon the Fair Information Practice Principles . . . .").

[7] *Id.*

[8] *See* 78 Fed. Reg. 13,026.

Obama Administration's commitment to civilian control of cybersecurity; (3) urge the release of documentation concerning purported cybersecurity authority for agencies, including the National Security Agency ("NSA"), involved in the Cybersecurity Framework, ; (4) distinguish between cybercrimes that fall under law enforcement and cyberterrorism that falls under national security; (5) acknowledge the 1992 OECD Guidelines for the security of information systems; and (6) fully adhere to the Privacy Act of 1974 and the Freedom of Information Act.

I. Ensure that Any Congressional Cybersecurity Legislation Includes Protections for Civil Liberties and Privacy

Any legislation on cybersecurity should have essential oversight and transparency mechanisms to ensure proper protection of privacy and civil liberties. As the Secretary of DHS, Janet Napolitano has said, "Congress should enact legislation to incorporate privacy, confidentiality, and civil liberties safeguards into all aspects of cybersecurity."[9] That same sentiment was recently echoed by Deputy Secretary of DHS, Jane Hall Lute.[10]

Legislation should provide added protections to ensure privacy and civil liberties are not compromised. For example, legislation can prevent the private sector from transferring personally identifiable information to the government. As the chairman of the Financial Services Information Sharing and Analysis Center recently noted in a House cybersecurity hearing, "much could be accomplished without *ever* sharing personally

[9] *The Cybersecurity Partnership Between the Private Sector and Our Government: Protecting our National and Economic Security: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs and S. Comm. on Commerce, Science, and Transportation joint hearing*, 113th Cong. 10 (2013) (statement of Janet Napolitano, Secretary of the U.S. Department of Homeland Security), *available at* http://www.hsgac.senate.gov/download/?id=bd6ad249-f43e-44ce-a369-5b23e39acf79.

[10] *DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure: Hearing Before the H. Comm. on Homeland Sec.*, 113th Cong. 10 (2013) (statement of Jane Hall Lute, Deputy Secretary of the U.S. Department of Homeland Security), *available at* http://docs.house.gov/meetings/HM/HM00/20130313/100390/HHRG-113-HM00-Wstate-LuteJ-20130313.pdf.

identifiable information."[11] Any exceptions to this rule should be limited and narrowly tailored. Also, Congress should prohibit the government from exploiting information for secondary uses that the government obtains from the private sector under the Cybersecurity Framework. Additionally, Congress should task the Privacy and Civil Liberties Oversight Board ("PCLOB") with overseeing cybersecurity implementation measures. Further, Congress should clarify and strengthen DHS's role as the government leader in cybersecurity efforts.[12]

Any cybersecurity legislation should be designed in a manner that does not discourage lawful, constitutionally protected activity. Protecting freedom of expression and association should be a paramount concern as our nation develops a cybersecurity policy, and care should be taken to ensure that new policies do not have a chilling effect on the expression of a wide diversity of ideas or association with others via the Internet. The Internet is a vital source of information for a large and growing number of citizens and is one of the primary platforms for the democratic discussion and debate necessary for a free society. First Amendment rights of expression and association are integrally connected to privacy, due process, equal protection, and indeed so are all the rights and values protected in the Bill of Rights. With respect to any cybersecurity legislation, NIST should urge Congress to include protections for privacy and civil liberties in line with the Cybersecurity Framework.

---

[11] *DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure: Hearing Before the H. Comm. on Homeland Sec.,* 113th Cong. 4-5 (2013) (statement of Anish Bhimani, Chairman of the Financial Services Information Sharing and Analysis Center) (emphasis added), *available at* http://docs.house.gov/meetings/HM/HM00/20130313/100390/HHRG-113-HM00-Wstate-BhimaniA-20130313.pdf.

[12] *See* Webcast: *DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure: Hearing Before the H. Comm. on Homeland Sec.*, 113th Cong. 10 (2013), http://mfile3.akamai.com/65736/wmv/sos1469-1.streamos.download.akamai.com/65740/chs_113th/03-13-13-full.asx.

II. Maintaining Civilian Control of Cybersecurity is Essential to Transparency, and All Agencies Involved Should Release Documentation for the Basis of Their Cybersecurity Authority

The need for transparency and public oversight underscores why cybersecurity efforts must be in the hands of a civilian agency. It is important that the government's cybersecurity efforts are subject to the transparency and oversight that comes with civilian agencies. Although the, for example, NSA's involvement for its expertise may be needed, in no way should the NSA covertly control cybersecurity or undermine the authority of DHS to run and lead the government's cybersecurity efforts. General Keith Alexander, the head of the U.S. Cyber Command and the National Security Agency, recognizes the need for a civilian agency to lead on cybersecurity and advises that DHS should be in the middle of any cybersecurity effort.[13] General Keith Alexander called putting civilian agencies in charge of domestic cybersecurity "the correct thing to do" because it allows "the transparency which I think the American People need in this area."[14]

Neither the NSA, nor any other non-civilian agency, should dictate cybersecurity efforts or become the de facto leader of cybersecurity behind the scenes. NSA has played an increasingly significant role in domestic communications security and concerns that the NSA may exert undo control and influence over cybersecurity efforts are legitimate. In a March 2009 resignation letter, Rod Beckstrom, the Director of the National Cybersecurity Center at the time, stated, "NSA effectively controls DHS cyber efforts through detailees, technology insertions, and the proposed move of NPPD and the NCSC

[13] Jennifer Martinez, *General: Nation Needs DHS involved in Cybersecurity*, The Hill Oct. 1, 2012, http://thehill.com/blogs/hillicon-valley/technology/259547-general-nation-needs-dhs-involved-in-cybersecurity.
[14] Transcript: Cyber Gridlock: Why the Public Should Care, 18 http://www.wilsoncenter.org/sites/default/files/cybersecuritytranscript.pdf .

to a Fort Meade NSA facility."[15] Mr. Beck continues, "NSA currently dominates most national cyber efforts."[16] While we respect the technical expertise of the Agency, it is vitally important that the American public can hold the government accountable for its actions within the field of cybersecurity.

The NSA has provided the public with little to no insight into the Agency's cybersecurity efforts, opting to remain a black hole for information on government cybersecurity efforts. Since January 2009, EPIC has pursued eight Freedom of Information Act matters with the NSA regarding its increasing role in domestic communications security. In six of those cases, the NSA has never disclosed documents responsive to EPIC's request. The NSA continually ignored the Freedom of Information Act's statutory deadlines or improperly refused to comply with required procedures. The NSA's actions in response to legitimate requests under the Freedom of Information Act have been evasive and undermine any thoughts that it will provide the needed transparency with respect to the government's cybersecurity efforts.[17]

The NSA has erected a wall of secrecy around its cybersecurity activity. As mentioned above, EPIC has spent enormous time and effort in an attempt to make the NSA's cybersecurity authority available to the public. EPIC has sought the text of National Security Presidential Directive 54, which sets forth NSA's role in cybersecurity and surveillance,[18] and Presidential Policy Directive 20,[19] which expands the NSA's

[15] Letter from Rod Beckstrom, Director, National Cybersecurity Center to Janet Napolitano, Secretary, Department of Homeland Security (March 5, 2009), *available at* http://online.wsj.com/public/resources/documents/BeckstromResignation.pdf.
[16] *Id*.
[17] *See* EPIC's letter to Senate for an overview of EPIC's efforts to acquire information about NSA's involvement in cybersecurity (sec. V.), *available at* http://epic.org/privacy/cybersecurity/EPIC-Senate-FOIA-Cybersecurity-Stmt-3-11.pdf.
[18] EPIC, Freedom of Information Act Appeal, FOIA Case 58987, *available at* http://www.epic.org/foia/NSPD54_complaint.pdf.

cybersecurity authority and has raised concerns about government surveillance of the Internet.[20]

Urging all agencies involved in cybersecurity, including the NSA, to release the documentation concerning their cybersecurity authorithy would provide the opportunity for meaningful public participation in the development of new security measures that may have a significant impact on civil liberties, such as privacy. The Senate Committee on Homeland Security and Governmental Affairs recognizes that cybersecurity initiatives must include actions to "…reassure [the public] that efforts to secure cyber networks will be appropriately balanced with respect for privacy and civil liberties."[21] EPIC urges NIST to encourage all agencies involved in the Cybersecurity Framework, including the NSA, to clarify their purported authority and role in cybersecurity.

The cybersecurity activity undertaken by the federal government must be carefully monitored and civilian control presents an opportunity to do this in a way military control does not. Any policies should be subject to the independent oversight of an empowered and effective Privacy and Civil Liberties Oversight Board. Additionally, cybersecurity efforts should be subject to rigorous public and congressional reporting as well as DHS Inspector General audits in order to protect individual liberties while providing robust cybersecurity.

[19] EPIC, Freedom of Information Act Appeal, *available at* http://epic.org/foia/nsa/NSA-PPD-Appeal.pdf.
[20] EPIC Complaint, *available at* http://www.epic.org/foia/FOIAapp112409.pdf.
[21] Letter from Joseph I. Lieberman, Chairman, and Susan M. Collins, Ranking Member, United States Senate Committee on Homeland Security and Governmental Affairs to Michael Chertoff, Secretary, Department of Homeland Security note 5 (May 1, 2008), *available at* http://hsgac.senate/gov/public/_files/5108LiebermanCollinslettertoChertoff.pdf.

III. The Cybersecurity Framework Should Distinguish Between Cybercrimes and Cyberterrorism

The overwhelming majority of cybersecurity incidents do not fall within the "national security" designation. As Deputy Secretary Lute has noted, cyberspace should not be managed like a warzone.[22] Most of the cybersecurity issues amount to civilian crimes committed in cyberspace (i.e. cybercrimes) that should be handled by state and local law enforcement and not under the rubric of national security.[23] The misappropriation of intellectual property, cyber-espionage, and hacktivism, to name a few cybersecurity issues, do not pose national security threats and should not be treated as such. The Cybersecurity Framework should narrowly focus on reducing "cyber risks to critical infrastructure,"[24] where critical infrastructure is statutorily defined as " systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[25] Only when cybersecurity incidents encompass this definition are they properly classified as cyberterrorism and fall under national security.

The Cybersecurity Framework should distinguish between those cybersecurity incidents that fall within the limited scope of national security (i.e. cyberterrorism) and those that do not (i.e. cybercrime). Too often claims of national security tip the

---

[22] *See* Webcast: *DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure: Hearing Before the H. Comm. on Homeland Sec.*, 113th Cong. 10 (2013) http://mfile3.akamai.com/65736/wmv/sos1469-1.streamos.download.akamai.com/65740/chs_113th/03-13-13-full.asx.

[23] *See* Webcast: *DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure: Hearing Before the H. Comm. on Homeland Sec.*, 113th Cong. 10 (2013) http://mfile3.akamai.com/65736/wmv/sos1469-1.streamos.download.akamai.com/65740/chs_113th/03-13-13-full.asx.

[24] Request for Information, 78 Fed. Reg. at 13,024.

[25] 42 U.S.C. § 5195c(e).

transparency-secrecy scale towards secrecy; thus the Cybersecurity Framework should clearly define what encompasses national security threats. Even those aspects of the Cybersecurity Framework that do fall under national security should be transparent whenever possible. As the National Security Strategy states, "our democracy depends upon transparency, and whenever possible we are making information available to the American people so that they can make informed judgments and hold their leaders accountable."[26]

IV. NIST Should Acknowledge the 1992 OECD Guidelines for the Security of Information Systems to Further Incorporate Privacy Protections

Privacy safeguards are vital to cybersecurity. Robust privacy protections promote cybersecurity in a number of ways. Proper privacy protections, including adequate data protection and avoidance of unnecessary transfers of personal information, limit exposure to a cyberattack or other type of breach and minimize the risk to individuals when such attacks occur.

Protecting individual privacy keeps cybersecurity efforts focused on robust efforts to secure cyberspace, prevent attacks, and minimize damage and disruption when attacks do occur. As noted, EPIC supports the Cybersecurity Framework's commitment to the FIPs. Further, in an effort to protect personal privacy and maintain the open and free flow of information, EPIC recommends the Cybersecurity Framework acknowledge the Organisation of Economic Co-operation Development ("OECD") Security Guidelines.[27]

[26] National Security Strategy 36-37 (May 2010), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[27] Organisation for Economic Co-operation Development, *OECD Guidelines for the Security of Information Systems Networks: Towards a Culture of Security* (1992), *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm.

These principles include:

- Accountability
- Awareness
- Ethics
- Multidisciplinary
- Proportionality
- Integration
- Timeliness
- Reassessment
- Democracy[28]

In particular, EPIC emphasizes the need for recognition of the Democracy Principle, which states "[t]he security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society."[29]

V. The Cybersecurity Framework Should Fully Adhere to the Privacy Act and Freedom of Information Act

The Cybersecurity Framework will provide an overarching structure for the U.S. Government's cybersecurity efforts. Those efforts may include the collection of personally identifiable information on individuals and any such collection is subject to the Privacy Act of 1974.

The Privacy Act of 1974 places extensive obligations on federal agencies that collect and use personal information.[30] The government's cybersecurity efforts should not be exempted from the obligations under the Privacy Act. In addition to the Privacy Act, all agencies involved in cybersecurity efforts should fully adhere to the openness requirements of the Freedom of Information Act ("FOIA"). The FOIA's purpose is to facilitate transparency by providing public oversight of government operations. Therefore agencies should only apply FOIA exemptions when they are absolutely necessary.

[28] *Id*.
[29] *Id*.
[30] 5 U.S.C. § 552a (2006).

VI. Conclusion

Agencies involved in the Cybersecurity Framework must uphold their obligations under the Privacy Act and the Freedom of Information Act. Every effort must be made to make cybersecurity policy transparent and to implement oversight mechanisms that provide accountability and protection for civil liberties and privacy. In refining the Cybersecurity Framework, NIST must, at a minimum: (1) ensure that any cybersecurity legislation includes protections for civil liberties and privacy; (2) abide by the Obama Administration's commitment to civilian control of cybersecurity; (3) urge agencies to release documentation concerning their purported cybersecurity authority; (4) distinguish between cybercrimes that fall under law enforcement and cyberterrorism that falls under national security; (5) acknowledge the 1992 OECD Guidelines for the security of information systems; and (6) fully adhere to the Privacy Act of 1974 and the Freedom of Information Act.

Respectfully Submitted,

Marc Roteberg
EPIC Executive Director

Amie Stepanovich
Director, EPIC Domestic Surveillance Project

Khaliah Barnes
EPIC Administrative Law Counsel

Jeramie D. Scott
EPIC National Security Fellow