December 13, 2013

Information Technology Laboratory
ATTN: Adam Sedgewick
National Institute of Standards and Technology
10 Bureau Drive, Stop 8930
Gaithersburg, MD 20899-9030

Re: Preliminary Cybersecurity Framework Comments

Dear Mr. Sedgewick:

The undersigned submit these comments in response to the National Institute of Standards and Technology's request for comments on the Preliminary Cybersecurity Framework [Docket No.: 130909789-3789-01].[1]

We applaud NIST for so carefully considering the significant privacy implications of the Cybersecurity Framework it is developing pursuant to Executive Order 13636.[2] We particularly appreciate that the proposed Appendix B acknowledges the importance of the Fair Information Practice Principles (FIPPs) for cybersecurity.[3] For decades, FIPPs have been applied to and accepted by a broad range of companies operating within critical infrastructure sectors as an effective and flexible way to protect consumers' privacy. Appendix B appropriately applies FIPPs to cybersecurity activities. Should it change in the final Cybersecurity Framework, it should nonetheless adhere to the eight tenets set forth in FIPPs.

Critical infrastructure companies that will be affected by the Cybersecurity Framework often hold internet data that 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; and cybersecurity initiatives should make protecting that privacy a paramount goal."[4]

---

[1] Nat'l Institute of Standard & Tech. Request for Comments on the Preliminary Cybersecurity Framework, 78 Fed. Reg. 64478 (proposed Oct. 29, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-10-29/pdf/2013-25566.pdf.

[2] Exec. Order 13,636, 78 F.R. 11,739 (Feb. 19, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[3] Nat'l Institute of Standard & Tech., Improving Critical Infrastructure Cybersecurity Executive Order 13636, App. B (2013), *available at* http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

[4] *DHS Cybersecurity: Roles and Responsibilities to Protect the Nation's Critical Infrastructure: Hearing Before the House Homeland Sec. Comm.*, 113th Cong. (2013) (statement of Michelle Richardson, Leg. Counsel, Washington Leg. Office, American Civil Liberties Union), at 1, *available at* http://docs.house.gov/meetings/HM/HM00/20130313/100390/HHRG-113-HM00-Wstate-RichardsonM-20130313.pdf.

Only full implementation of the FIPPs will sufficiently protect Americans' privacy and security. Moreover, adherence to the FIPPs will promote confidence in the critical infrastructure companies that hold, and must safeguard personal information, while still ensuring that companies have the tools they need to effectively protect their networks. Using FIPPs as a baseline for privacy practices will also build a common environment where different companies that are collecting and handling the same types of Personally Identifiable Information (PII) will adhere to the same sets of privacy principles and rules. To prevent unwarranted privacy risks, NIST should recommend in Appendix B of its Cybersecurity Framework that each critical infrastructure company follow a comprehensive privacy and data protection policy. In brief, NIST should directly reference the eight FIPPs:

- **Transparency:** Critical infrastructure companies should create and make publicly available a data collection policy that explains the PII that is being collected, as well as how it may be used, disseminated, and maintained. Additionally, on a regular basis, companies should prepare a public report on the types of PII collected and catalog any privacy incidents that occurred during the reporting period.
- **Individual Participation:** Critical infrastructure companies should, to the extent practicable, seek consent from individuals whose PII may be collected, used, disseminated, or maintained. To the extent practicable, critical infrastructure companies should also notify individuals whose information has been collected, used, disseminated, or maintained; and provide those individuals with "mechanisms for appropriate access, correction, and redress regarding use of PII."[5]
- **Purpose Specification:** PII should be collected, used and disseminated pursuant to specific, articulated cybersecurity purposes. Critical infrastructure companies should inform the affected individuals of the purpose of the collection, use, and dissemination of their PII.
- **Data Minimization:** Critical infrastructure companies that collect data for cybersecurity purposes should only store the PII that is clearly needed for cybersecurity purposes, and should not store data for longer than is necessary. Companies should set concrete standards for the duration of data retention and ensure that PII is deleted after that time.
- **Use Limitation:** Use of collected PII should not exceed the purposes set forth in the critical infrastructure company's publicly available data collection policy, or as otherwise necessary to protect the company's networks.
- **Data Quality and Integrity:** Critical infrastructure companies should ensure that any PII collected is "accurate, relevant, timely, and complete."[6] Companies have a duty to ensure that the information collected has not been altered or destroyed in an unauthorized manner and that, to the extent practicable, affected individuals have the ability to correct inaccuracies in the PII collected and maintained for cybersecurity purposes.
- **Security:** Data collection statements and test plans should detail the security used for information sharing with the government and other private sector companies.
- **Accountability and Auditing:** All employees should be familiar with their company's privacy policy and the Chief Information Officer (CIO) or other appropriate manager

[5] White House, National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy: Enhancing Online Choice, Efficiency, Security, and Privacy, App. A (Apr. 2011), available at http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.
[6] Id.

should ensure that employee behavior is in line with that policy. The CIO or appropriate manager should audit employee performance on a randomized basis to ensure that the privacy policy is being strictly followed. Where required by law, individuals should be notified if their personal information is improperly accessed, used, or otherwise compromised.

Appendix B of the Cybersecurity Framework captures these FIPPs concepts. Mapping the FIPPs concepts to the elements of the Framework core, as Appendix B does, will ensure that FIPPs are accounted for and complied with as critical infrastructure companies engage in the activities contemplated in the Framework core. But, it is not the only way that FIPPs could be incorporated in the Framework. It would, for example, be entirely appropriate for NIST to signal in Appendix B that its goal is for companies to adopt data practices that comport with the FIPPs and that NIST's articulation in Appendix B of those activities is meant to be flexibly applied. In addition, Appendix B should explicitly state that the informational references provided are for guidance only and that NIST recognizes that some aspects of those references would apply only to governmental activities (such as issuing System of Records Notices) and not to the activities of companies in the private sector.

While we believe that some flexibility is warranted, we urge NIST to reject the invitation that it water down the role of FIPPs in the framework. Other commenters have urged NIST to adopt primarily process-based protections without adequately integrating FIPPs principles into the processes that would be put in place.[7] However, this is inconsistent with the rest of the Framework, which envisions both processes and outcomes. Processes are adopted to reach an outcome and full application of the FIPPs principles in the Framework informs those outcomes. Because protecting individual privacy in the cybersecurity context is so important to the success of the Framework, instituting strong, FIPPs-based protections will ultimately benefit the private sector companies that adopt the Framework and will give the public confidence that they can entrust data to those companies.

In conclusion, we urge NIST to issue a final Framework that envisions critical infrastructure companies adherence to FIPPs, and that it signal in Appendix B some flexibility with respect to the informative references that are made. Adherence to FIPPs will help ensure that companies can effectively defend their networks from cyberattacks and at the same time, protect the privacy of the PII that is used in such defense.

Sincerely,

Access
Advocacy for Principled Action in Government
American Civil Liberties Union
American Library Association
Arab American Institute

[7] Letter from Harriet P. Pearson, Partner, Hogan, Lovells US LLP, to Adam Sedgewick, Nat'l Institute of Standards & Tech. (Dec. 5, 2013) (on file with author), *available at* http://csrc.nist.gov/cyberframework/framework_comments/20131205_harriet_pearson_hoganlovells.pdf.

Center for Democracy & Technology
Center for National Security Studies
Center for Rights
Citizens for Responsibility and Ethics in Washington
The Constitution Project
Defending Dissent Foundation
Electronic Frontier Foundation
Fight for the Future
New America Foundation's Open Technology Institute
PolitiHacks