April 8, 2013

National Institute of Standards and Technology
U.S. Department of Commerce
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Re: National Institute of Standards and Technology: "Developing a Framework to Improve Critical Infrastructure Cybersecurity"

In response to the National Institute of Standards and Technology (NIST) Request for Information on *Developing a Framework to Improve Critical Infrastructure Cybersecurity,* The Constitution Project submits these comments regarding protection of privacy and civil liberties as part of the Framework.

The Constitution Project (TCP) is a nonprofit organization in Washington, DC that promotes and defends constitutional safeguards by bringing together liberals and conservatives who share a common concern about preserving civil liberties. The Constitution Project's bipartisan Liberty and Security Committee, launched in the aftermath of September 11th, brings together members of the law enforcement community, legal academics, former government officials, and advocates from across the political spectrum who develop and advance proposals to protect civil liberties as well as our nation's security.

As part of this work, TCP's Liberty and Security Committee released a report in 2012 entitled *Recommendations for the Implementation of a Comprehensive and Constitutional Cybersecurity Policy*.[1] This report urges the government to ensure that we protect individuals' privacy interests and proposes specific recommendations for measures to incorporate civil liberties safeguards into government cybersecurity programs.

In general, the Cybersecurity Framework to be created pursuant to Executive Order 13636 poses far fewer threats to privacy and civil liberties than would proposed cybersecurity legislation, for the simple reason that the Executive Order does not, and cannot, create exemptions from existing privacy protective statutes. Nonetheless, any information sharing program can create risks for Americans' privacy rights and civil liberties, and therefore TCP welcomes NIST's recognition that the Framework must include measures to protect privacy and civil liberties. This includes the statement in the Request for Information that the menu of management, operational and technical security controls should include measures to protect privacy and civil liberties, as well as the provision that the Framework itself should include a "menu of privacy controls necessary to protect privacy and civil liberties."

[1] An electronic copy of *Recommendations for the Implementation of a Comprehensive and Constitutional Cybersecurity Policy* can be found at the Constitution Project's website, at http://www.constitutionproject.org/wp-content/uploads/2012/09/TCPCybersecurityReport.pdf

NIST proposed numerous specific questions in its Request for Information. The questions regarding current risk management practices and those regarding current use of frameworks and guidelines for industry are beyond the scope of TCP's cybersecurity report and the issues addressed by TCP's Liberty and Security Committee. Based upon TCP's Liberty and Security Committee's cybersecurity report, the comments below address NIST's questions regarding the risks that industry practices pose to privacy and civil liberties.

In response to NIST's questions about the risks to privacy and civil liberties created by specific industry practices and about how to manage such risks, TCP submits the following recommendations:

Follow Fair Information Practice Principles: Executive Order 13636 provides that in implementing the order, federal agencies should follow the Fair Information Practice Principles (FIPPs). This commendable requirement should also be applied to the development of the Framework itself. The risks to privacy and civil liberties posed by the practices set forth in the final Framework should be assessed and mitigated following the FIPPs. In particular, the Framework should incorporate measures to promote data minimization, use limitations for private information, protections for data integrity, and accountability and auditing requirements.

Minimize Sharing of Private Information: Although the Framework and the information sharing program created under the Executive Order are voluntary for private industry, the Framework should include provisions to encourage private businesses to minimize the review and sharing of personally identifiable information (PII) and the content of private communications. This should include a provision stating that when companies share cyber threat information with each other or with the government, they should make "reasonable efforts" to remove PII and private information that is unrelated to the cyber threat. The Framework's guidance on best practices should include methods for achieving such minimization of PII and the content of private communications, including guidance on possible automated processes.

Limit Data Retention: The Framework should provide that when data collected for cybersecurity purposes includes PII or the content of private communications, there should be strict time limits for data retention. PII and the content of private communications that are not relevant to any cyber threat should be purged promptly.

Limit the Uses of Private Information: To the extent that the Framework provides for or encourages private companies to share cyber threat information with the government, the program should strictly limit the uses of such shared private information to cybersecurity purposes, including the investigation and prosecution of cybersecurity crimes. Government should not be permitted to use cyber threat information containing PII or the content of private communications for purposes beyond cybersecurity. Information collected for cybersecurity purposes should not be shared with law enforcement officials for non-cybersecurity purposes or relied upon as evidence of a non-cyber crime, unless law enforcement first obtains a warrant based on a showing of probable cause.

Data Safeguards Should Include Privacy Safeguards: Standards adopted to safeguard databases and data integrity, should include policies and best practices for employing data anonymization whenever possible as well as policies to diminish the risk of inadvertent or improper disclosure of information containing PII.

Incorporate Accountability and Auditing Requirements: The Framework should provide for regular audits to promote accountability. The audits should assess the overall effectiveness of the program and should specifically measure whether privacy and civil liberties safeguards are sufficiently robust and are being implemented properly.

The Constitution Project encourages NIST to rely upon the FIPPs to incorporate robust safeguards for privacy and civil liberties into the Framework.

Respectfully submitted,

Sharon Bradford Franklin
Senior Counsel
The Constitution Project
1200 18th Street, NW
Suite 1000
Washington, DC 20036