usacm ACM US Public Policy Council

RESPONSE TO REQUEST FOR INFORMATION
Cybersecurity Framework
78 FR 13024
DOCUMENT NUMBER 2013-04413
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

RESPONSE FILED BY:
U.S. PUBLIC POLICY COUNCIL OF THE ASSOCIATION FOR COMPUTING MACHINERY

On behalf of the U.S. Public Policy Council (USACM) of the Association for Computing Machinery (ACM) we are submitting the following comments in response to the Request for Information by the National Institute for Standard and Technology on the Cybersecurity Framework ("Framework") set forth in Executive Order 13636.

With over 100,000 members, the Association for Computing Machinery (ACM) is the world's oldest and largest educational and scientific computing society. The ACM U.S. Public Policy Council (USACM) serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology. Our comments are informed by the research experience of our membership. Should you have any questions or need additional information, please contact our Public Policy Office at 212-626-0541 or at acmpo@hq.acm.org.

We welcome the effort to establish – through the Framework – a collection of guidelines, methodologies, procedures and processes to help critical infrastructure stakeholders work toward our shared cybersecurity goals. We're especially encouraged by the inclusion in the Framework of standards, guidelines, and best practices that provide "a menu of privacy controls necessary to protect privacy and civil liberties." Ensuring effective protection of personal and sensitive information helps protect privacy and civil liberties, but the benefits do not stop there. Applying the Fair Information Practice Principles to data collection and sharing systems like the one that the Framework will support can help preserve the security and reliability of the system as well.

The potential damage from exposure of sensitive information (whether it is personally identifiable, proprietary and/or confidential) represents a serious security risk in and of itself. Such information may provide the basis for embarrassment, blackmail, intimidation or increased risk of social engineering attacks on individuals who have had their information exposed. Exposure of proprietary and/or confidential business information in a shared environment exposes companies to risk of similar attack, as well as possible unfair business practices.

Recognizing the need for the sharing of such information, great care should be taken to control its access and use by the government as well as those parties with whom the information is shared. Section 5(d) of the Executive Order

> "Information submitted voluntarily in accordance with 6 U.S.C. 133 by private entities under this order shall be protected from disclosure to the fullest extent permitted by law."

is important guidance, but specific steps must be taken to help minimize the risk of inappropriate disclosure. In particular, access controls, data minimization and other Fair Information Practices should be considered to avoid circumventing existing legal limits on government access to this information. These practices can also make data management easier by reducing the amount of extraneous information collected. While parties may feel like erring on the side of disclosing more information rather than less, that choice can have adverse consequences. These consequences can include exposing personal and/or business information that competing and/or malicious entities may use to their advantage. This potential for harm to those who may wish to share threat information is a disincentive to such sharing.

NIST should set up a Framework that acknowledges both the fluidity of cybersecurity and the variety of cybersecurity needs in various sectors. A key challenge to NIST encouraging the establishment of standards and conformity assessment testing is the speed by which new cybersecurity challenges and responses to those challenges emerge. This dynamic is significantly different from the challenges facing most other proposed standards projects. We propose that NIST invite contributions on how the effectively address this situation. To the extent that standards are going to be part of the Framework, we would encourage those standards to be sector-specific, or sufficiently narrow that the standard can be evaluated to demonstrate that it increases security for the covered systems.

Additionally, the Framework should include as many tools, guidelines, and other resources to encourage the design, development and implementation of cybersecurity from the time a system becomes operational. Programs like the Build Security In initiative that help build secure software are aimed at this objective, and should be included in the Framework.

Answers to specific questions in the RFI

Current Risk Management Practices

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

Unfortunately, the field of cybersecurity is not mature enough, compared to other fields, to rely on standards setting and conformance to accomplish security goals. The security and safety of other goods and services can be relied on if they conform to established standards. But for cybersecurity such a conformance process risks locking in systems to a cybersecurity environment of a specific point in time.

Specific Industry Practices
9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

Our answer is focused on the application of the practices referenced in the RFI in the context of information sharing with the government and other entities.

Information security and privacy are not tradeoffs to be balanced, but interrelated goals to be pursued. It is important to note that the application of at least some of the practices outlined in this section (encryption, key management, access controls, security engineering practices) can strengthen privacy and civil liberties protections by minimizing the risk of information exposure. Securing the confidentiality of private sector and personal information will strengthen privacy as well as security.

The application of Fair Information Practice Principles (FIPPs) could run into conflict with two kinds of practices outlined in the RFI: monitoring and incident detection tools and capabilities and incident handling policies and procedures. As cyber attacks become increasingly sophisticated by combining a range of techniques, including social engineering, the evidence needed to detect and share threat information will increasingly include personal information, such as e-mail, web browser history, and other personal data. The conflict arises when this information is shared with government and intelligence agencies pursuant to section 5(d) of the Executive Order. Strong data minimization practices implemented prior to information sharing, including steps to de-identify personally identifiable and otherwise sensitive information, may minimize the risk of this type of conflict.

11. How should any risks to privacy and civil liberties be managed?

Part of effective risk management is establishing processes and procedures for analyzing and mitigating risks to privacy and civil liberties as part of the Framework. The FIPPs should be used as a floor or a minimum standard. The FIPPs are context dependent and a concise means of specifying purposes and ensuring that data sharing occurs within the limits of purpose specification would help manage privacy and civil liberties risks. Tools that can help in this process include a dataflow-based lexicon. This is a compendium of standard representations of how personal information flows between different entities in the context of a particular purpose, such as the sharing of cybersecurity threat information for national security purposes. These tools can help reduce re-purposing of information, which is one precursor to privacy harm.

Privacy impact assessments (PIAs) and risk models that factor in specific threats to personal privacy are useful tools to help manage privacy and civil liberties risks. While PIAs are often descriptive, they can and should also be used as analytical tools, wherein data flows are described and corresponding privacy risks are assessed in tandem. PIAs can have greater analytic capabilities if they include privacy risk models that enable analysts to plan for and respond to potential privacy harms by proposing appropriate risk management strategies (mitigation, avoidance, etc.).

We explained the lexicon and the use of privacy impact assessments in additional detail in our comments to the National Telecommunications and Information Administration[1] on an Internet Privacy Task Force report. We refer you to that document for additional details.

[1] http://www.ntia.doc.gov/files/ntia/comments/101214614-0614-01/attachments/Commerce_Department_Online_Privacy_Comments_USACM.pdf