Association for Computing Machinery (ACM)
US Public Policy Council of ACM (USACM)

usacm.acm.org
facebook.com/usacm
twitter.com/usacm

RESPONSE TO THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Request for Information
Experience with the Framework for Improving Critical Infrastructure Cybersecurity
Document Number 2014-20315
79 FR 50891

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

We submit the following comments on behalf of the U.S. Public Policy Council (USACM) of the Association for Computing Machinery (ACM).

ABOUT ACM AND USACM

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.

General Comments

USACM submitted comments on the Cybersecurity Framework in April 2013,[1] prior to the development of Framework version 1.0 and the accompanying Roadmap. We stand by our comments from that time and encourage the National Institute of Standards and Technology (NIST) to make sure that any changes to the Framework and Roadmap help minimize the risk of inappropriate disclosure of information. In particular, we re-emphasize our concerns from the 2013 comments on the need to resist disclosing too much information. As we said in those comments:

> "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

[1] http://csrc.nist.gov/cyberframework/rfi_comments/040813_usacm.pdf

information is a disincentive to such sharing."

Ensuring that the proper kind and amount of information is shared is important for privacy and security considerations. It is also relevant to the effectiveness of the goals of the Framework – sharing meaningful cybersecurity information with the parties that can benefit from it the most.

Answers to specific questions in the Request

Roadmap for the Future of the Cybersecurity Framework

1. Does the Roadmap identify the most important cybersecurity areas to be addressed in the future?

The Roadmap does identify several important cybersecurity areas for the future. In particular, the discussion of Technical Privacy Standards in Section 4.9 lines up well with the NIST efforts embodied in its privacy engineering workshops and should be an important part of the Framework and the Roadmap moving forward. We recommend that future editions of the Roadmap and Framework determine where areas of cybersecurity and cyber safety could be usefully integrated.

Additionally, the Roadmap should identify areas within Section 4 that could productively inform each other. For instance, Technical Privacy Standards (Section 4.9) can and should be integrated with Data Analytics (Section 4.5) and with the development of the Cybersecurity Workforce (Section 4.4). Those standards would be important things for the future workforce to learn.

2. Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?

The role of autonomous devices in the energy and health care sectors deserves priority consideration. The cybersecurity of devices like smart meters, wirelessly networked medical devices, and similar items that rely on networking to communicate information in these sectors does not have effective, consistent guidance from relevant regulatory entities. These items are part of the emergent Internet of Things, and the role of these autonomous devices within energy and health care systems is important enough for them to be considered critical infrastructure. If they fail or are exploited, the potential consequences for the systems that rely on these devices, as well as for the safety and welfare of the individuals using and/or relying upon them, are significant.

3. Have there been significant developments—in the United States or elsewhere—in any of these areas since the Roadmap was published that NIST should be aware of and take into account as it works to advance the usefulness of the Framework?

As mentioned above (and in the Roadmap), NIST's efforts in privacy engineering[2] should be considered when advancing the usefulness of the Framework. Work being done in the Identity Ecosystem Steering Group[3] - which is the entity responsible for making the National Strategy for Trusted Identities in Cyberspace a reality – should also inform the Framework (and IDESG meetings may serve as opportunities to promote the Framework).

The National Telecommunications and Information Administration is working to facilitate multistakeholder-derived voluntary codes of conduct on consumer privacy. That work is worth reviewing as it faces similar challenges in encouraging voluntary adoption of best practices.

---

2 http://www.nist.gov/itl/csd/upload/nist_privacy_engr_objectives_risk_model_discussion_draft.pdf

3 http://www.idecosystem.org