January 19, 2018
Submitted to cyberframework@nist.gov

**Comments on "Framework for Improving Critical Infrastructure Cybersecurity" Version 1.1 Draft 2 Before the National Institute of Standards and Technology**

Thank you for this opportunity to respond to the National Institute of Science and Technology (NIST) Request for Public Comment on the Framework for Improving Critical Infrastructure Cybersecurity (Framework).[1] Access Now commends NIST for draft changes that will improve the Framework, in particular by expanding on coordinated vulnerability disclosure and authentication. Implementation of vulnerability disclosure programs and authentication tools will improve security of the organizations and better protect the privacy of stored user data. Areas for additional exploration in future versions need careful consideration, with attention paid to the impact on user rights, including privacy.

Access Now defends and extends the digital rights of users at risk around the world. Access Now advocates for cybersecurity policies that are **user centric**, **systemic**, and anchored in **open and pluralistic process**. We seek to strengthen human rights protections in cybersecurity policies, support the development of coordinated vulnerability disclosure processes, safeguard the role of security researchers, and to promote high standards to protect users with respect to the Internet of Things and emerging technologies.

Below, we lend support to improvements made in the draft Framework, including vulnerability disclosure, and urge their inclusion in the final version of the Framework. We then address areas for future development identified in the "Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1" (Roadmap), including Identity Management, Privacy Engineering and International Aspects, Impacts, and Alignment.

*Vulnerability Disclosure*

The very nature of technology guarantees the existence of vulnerabilities. The further integration of technology into our lives increases the impact of vulnerability exploitation. The addition of subcategory RS.AN-5 will promote the adoption and stronger implementation of coordinated vulnerability disclosure programs to "receive, analyze and respond" to vulnerabilities, thus decreasing the risk of exploitation and threats to individual users. Effective implementation under the Framework should discourage misuse of bug bounty programs to conceal breaches of private customer data, as seen in at least one instance in 2017.[2]

[1] https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_with-markup.pdf

[2] https://www.forbes.com/sites/forbestechcouncil/2018/01/11/bug-bounty-ethics-in-the-aftermath-of-the-uber-breach/#7957ca6a5a86

Access Now joined Rapid 7 and other organizations in a separate letter commending NIST for the inclusion of RS.AN-5 and calling for reference to additional standards to improve the implementation of coordinated disclosure programs.[3]

*Identity Management, Authentication and Access Control*

The inclusion of a subcategory on authentication (PR.AC-7) demonstrates the value of authentication methods. We encourage NIST to maintain the subcategory in the final version and to expand on authentication in future versions of the Framework. The failure of authentication methods to protect against attack has been a significant factor in data breaches, many of which have resulted in the compromise of passwords from user accounts further imperiling account integrity.[4] Promoting the institutional adoption of authentication tools will help protect against theft of user data while increasing their profile. Access Now has recommended users enable multi-factor authentication wherever it is supported and provided resources on available options.[5]

The Roadmap recognizes the risks of stolen and weak passwords and describes biometrics as an area for future exploration for identity management.[6] The benefits and risks of biometrics must be fully explored, with adequate public input, before integration into the Framework. Biometrics can be easier and quicker to use than passwords or other methods of authentication. The use and storage of biometrics, however, can pose privacy risks. Because biometrics are static, a breach of biometric data can have permanent consequences.[7] If a password (or a Client Certificate or OTP device, etc.) is compromised, it can be changed or reset; the options for mitigating this risk with biometrics are limited.

*International Aspects, Impacts, and Alignment*

The Roadmap identifies the use of the Framework "to efficiently operate globally" given that countries "are working to develop their own, unique standards and best practices which may make interoperability at the international level a more challenging and sometimes onerous process." International coordination between NIST and other national cybersecurity and data protection bodies can promote improved cybersecurity. However, the Framework should not serve as a replacement for policies that improve security accountability, protect human rights, and improve accountability. The Framework is a useful tool to compare to cybersecurity laws

---

[3] https://www.rapid7.com/globalassets/_pdfs/rapid7-comments/joint-comments-to-nist-framework-revision-1.1.2-rapid7-011918.pdf

[4] *See* https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/; http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html

[5] https://www.accessnow.org/cms/assets/uploads/2017/09/Choose-the-Best-MFA-for-you.png

[6] https://www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf

[7] https://www.scmagazineuk.com/biometrically-challenged-three-factor-authentication-systems-too-weak-for-web-banking/article/530568/

that seek to increase government control of user data.[8] In Europe, however, the Directive on the Security of Network and Information Systems (NIS Directive) and General Data Protection Regulation (GDPR) impose and will soon impose on companies legal liabilities beyond those in the U.S. that improve security and accountability. NIST and other entities that promote the Framework internationally should seek to support and supplement such efforts.

*Privacy Engineering*

The draft Framework continues to recognize the relationship between cybersecurity and privacy and civil liberties, specifically the risks cybersecurity programs can pose. However, the civil liberties language in the draft Framework Core should be strengthened. The Roadmap rightfully acknowledges the limitations of the "Fair Information Practice Principles" (FIPPS) and the need for more research into privacy engineering. Access Now supported the NIST report on privacy engineering ("An Introduction to Privacy Engineering and Risk Management in Federal Systems") and called for the private sector to implement the recommendations.[9] The draft Framework should be strengthened to inform companies they "should" or "must" rather than "may" consider how cybersecurity programs might incorporate privacy practices. That alone is not enough. Civil society organizations have developed a plethora of resources to help organizations better protect user security and rights.[10] The Framework Core Subcategory ID.GV-3 should be strengthened to include such resources.

The draft  Framework is an improvement over previous versions. However, there is more to be done. As NIST considers what changes to make in the next iteration of the Framework, we encourage greater consideration of the intimate relationship between organizations' cybersecurity and the the security and rights of their users.

For more information, please contact,

Drew Mitnick
Policy Counsel

Amie Stepanovich
U.S. Policy Manager and Global Policy Counsel

[8] https://www.accessnow.org/understanding-chinas-cybersecurity-law-flawed-design/; https://www.accessnow.org/transparency-reporting-index/
[9] https://www.accessnow.org/new-report-helps-u-s-federal-agencies-protect-privacy-companies-use/
[10] *See e.g.* https://www.encryptallthethings.net/