Dr. Willie E. May
Acting Director
National Institute for Standards and Technology
100 Bureau Drive, Stop 1070
Gaithersburg, MD 20899-1070
wem@nist.gov

William Polk
Group Manager, Cryptographic Technology Group
National Institute for Standards and Technology
Computer Science Division
william.polk@nist.gov

Matthew Scholl
Acting Division Chief & Deputy Division Chief
National Institute for Standards and Technology
Computer Science Division
matthew.scholl@nist.gov

Dr. Lily Chen
Group Manager (Acting), Cryptographic Technology Group
National Institute for Standards and Technology
Computer Science Division
lily.chen@nist.gov

cc: President Barack H. Obama
The White House
1600 Pennsylvania Ave.
Washington, D.C. 20500

cc: Megan Smith
U.S. Chief Technology Officer
Office of Science and Technology Policy
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Ave.
Washington, D.C. 20504

cc: Penny Pritzker
Secretary of Commerce
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, D.C. 20230
PPritzker@doc.gov

November 20, 2014

To Whom It May Concern:

We, the undersigned companies and civil society organizations, are writing to re-emphasize the importance of creating a process for establishing secure and resilient encryption standards, free from back doors or other known vulnerabilities. NIST is currently preparing the final version of its

Cryptographic Standards and Guidelines Development Process.[1] In order to restore trust and re-commit itself to the promotion of innovation and industrial competitiveness, NIST must make a strong statement ensuring independence, security, and integrity.[2] Below we renew our initial recommendations for the finalization of this document, add additional recommendations in support of an open and accountable NIST, and call on NIST to conduct outreach with members of civil society and privacy experts to establish an ongoing dialogue on these important matters.

In September 2013, the public learned that the National Security Agency (NSA) abused its consultative authority with NIST to artificially lower encryption standards. In the wake of these revelations, civil society has repeatedly called on NIST to increase transparency and accountability in its encryption standards-setting process. These activities by the NSA have already had a measurable impact on the U.S. economy and have resulted in the global distrust of U.S.-led encryption standards.[3] While we commend you on the progress made so far, we urge that much more must be done to restore the public's trust in the agency and to ensure that secure communications tools and technologies are built on solid foundations.

In October, NIST cryptologist and mathematician Andy Regenscheid presented at the Information Security and Privacy Advisory Board's meeting, providing an update on the status of NIST's review of its cryptographic standard-setting process.[4] Mr. Regenscheid emphasized the importance of full transparency and reiterated NIST's pledge that "all [NSA] contributions to NIST guidance will be acknowledged."[5] In April a coalition of organizations and companies responded to a draft of the NIST Cryptographic Standards and Guidelines Development Process and call on the NIST to "establish a policy wherein the agency publicly explains the extent and nature of the NSA's consultation on future standards and any modifications thereto made at NSA's request."

Mr. Regenscheid's statement stands as a great first step toward recognition of this much-needed transparency, as is NIST's on-the-record commitment to hire more internal cryptographers and to increase engagement with the academic community.[6]

---

[1] VISITING COMMITTEE ON ADVANCED TECHNOLOGY OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS (2014), *available at* http://www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf [hereinafter *VCAT Report*].

[2] MISSION, VISION, CORE COMPETENCIES, AND CORE VALUES, http://nist.gov/public_affairs/mission.cfm (last visited Nov. 14, 2014).

[3] NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE, SURVEILLANCE COSTS: THE NSA'S IMPACT ON THE ECONOMY, INTERNET FREEDOM & CYBER SECURITY (2014), *available at* http://oti.newamerica.net/sites/newamerica.net/files/policydocs/Surveilance_Costs_Final.pdf.

[4] Tal Kopan, *N.Y. Financial Chief Eyes Cybersecurity – Scoop: Rockefeller Wants Answers From Whisper – Energy Sector a Cautionary Tale on Cyber Regulation*, POLITICO (Oct. 23, 2014, 10:02 AM EDT) http://www.politico.com/morningcybersecurity/1014/morningcybersecurity15793.html.

[5] VCAT Report, *supra* note 1, at 17.

[6] *Id.*

However, these first steps only underscore how little has been done in the past fourteen months to rectify NIST's trust deficit. NIST has not publicly acknowledged several other coalition recommendations, namely:

1. "NIST should further commit, to the extent that it does not invade personal privacy interests, to transparency on the identity and affiliation of individuals and organizations that consult on the development process.";
2. "NIST should establish a policy wherein the Agency publicly explains the extent and nature of the NSA's consultation on future standards and any modifications thereto made at NSA's request" and "NIST should begin a review process to ensure that wherever possible the same information is published for standards that are currently in use.";
3. "NIST should attempt to maximize reach and engagement and limit barriers to access in order to conduct the best possible outreach to the public" and further, "[i]n deciding on platforms, NIST should not only consider reach, level of engagement, and barriers to access, but also the ability to search for and access historical content to ensure persistence and continuity.";
4. "NIST should commit to always providing a security proof for standards when the standard is put out for public comment" and "to explaining the justification for, origin, and means of generation for any parameters supplied in NIST standards.";
5. "[NIST] should specify that, unless necessary, [the Agency] will only take into account information assurance needs of government in establishing cryptography standards, and should, under no circumstances, consider the signals intelligence needs of the NSA or any other intelligence or law enforcement need of any agency."; and
6. "NIST should extend [the principle of Usability] to its cryptography work to ensure that security standards are not weaker in practice than anticipated by examining only the underlying mathematics.".[7]

These recommendations were heavily echoed in the reports submitted by the members of NIST's appointed Committee of Visitors (CoV). The CoV is a distinguished panel of experts appointed by NIST's own Visiting Committee on Advanced Technology (VCAT), a group that makes policy recommendations to NIST. The CoV included seven experts, including Edward Felten, Ronald Rivest, and Frances E. Schrotter, each of whom submitted their own report and recommendations. In more than 81 total recommendations, the experts unambiguously called for greater accountability and independence for the agency. Internet pioneer Vint Cerf stated in his report, "NIST cannot be seen as nor be subject to any kind of coercion or veto by the National Security Agency."[8]

[7] Letter from Coalition to Crypto-Review at the National Institute of Standards and Technology (April 18, 2014), *available at* https://s3.amazonaws.com/access.3cdn.net/73934b6b48cbc48268_oim6bx0jn.pdf.
[8] VCAT report, *supra* note 1.

In addition to the recommendations above, the below-signed would like to endorse several additional recommendations that appeared as common themes throughout the several CoV reports:

1. NIST must publicly and irrefutably commit itself to independence from the NSA's signals intelligence mission and any government surveillance programs, activities, or authorities;
2. NIST must expand to include independent full-time technical expertise and additional funding in order to decrease reliance on the NSA and other members of the Intelligence Community. To the extent that an Act of Congress is necessary to achieve these items, NIST should provide a well-researched, public budget request, which identifies the amount of funding that the Agency currently receives through appropriations from other agencies, and should call on Congress to take immediate action to approve the request;
3. NIST should revisit and revise its Memorandum of Understanding (MOU) with the NSA. The MOU was first entered into between the two agencies in 1989, and was amended in 2010.[9] The MOU should again be amended, not only to recognize NIST's commitment to transparency on consultations with the NSA, but also to add express limitations on that consulting. The MOU should expressly limit NSA's consultations to the furtherance of its Information Assurance mission,[10] and any consultation that artificially lowers encryption standards to preserve signals intelligence capabilities must be expressly prohibited;[11] and
4. Several members of the CoV recommended establishing a permanent advisory board or committee for overseeing and assisting with standards processes and auditing. NIST should immediately investigate the implementation of such an advisory board and provide a public report on its feasibility and potential role with the agency. Upon the completion of the investigation and report, the NIST should pursue establishment of such an advisory board.

These additional recommendations are necessary to respond to the continued public outcry over the agencies' collaboration.

Finally, NIST should establish and facilitate a continued dialogue with members of civil society, advocacy organizations, and other experts who represent the interests of the general public and users. NIST's processes and procedures are highly technical and rely on a significant level of

[9] Memorandum of Understanding Between the Director of the National Institute of Standards and Technology (NIST) and the Director of the National Security Agency (NSA) Concerning the Implementation of the Federal Information Security Management Act of 2002 (Dec. 23, 2010), *available at* http://csrc.nist.gov/groups/ST/crypto-review/documents/NIST_NSA_MOU-2010.pdf [hereinafter MOU]
[10] ABOUT IA. AT NSA, NAT'L SEC. AGENCY, http://www.nsa.gov/ia/ia_at_nsa/ (last visited Nov. 14, 2014).
[11] See, e.g., H.Amdt. 930 to H.R.4870, 113th Cong. (2014) ("An amendment, offered by Mr. Grayson, to prohibit the use of funds to "consult", as the term is used in reference to the Department of Defense and the National Security Agency, in contravention of the assurance provided in section 20(c)(1)(A) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3(c)(1)(A)"), *available at* http://clerk.house.gov/floorsummary/floor.aspx?day=20140619&today=20140619.

pre-existing knowledge in order to adequately participate. Civil society organizations bridge the gap between government agents and the public in order to provide important feedback for all parties involved. Other branches of NIST have recognized this and have involved civil society in public workshops to explore pressing topics and issues.[12] NIST's encryption standards impact the daily lives of users around the world on a frequent basis — civil society should be a central part of the conversations.

Thank you for your attention to these urgent matters. If you have questions or concerns regarding the content of this letter, please contact Amie Stepanovich with Access at amie@accessnow.org or +1.888.414.0100 ext. 702 and she will communicate with the other signatories.

Sincerely,

Access
Advocacy for Principled Action in Government
AeroFS
American Library Association
Citizens for Responsibility and Ethics in Washington (CREW)
Cloudflare
Computer & Communications Industry Association (CCIA)
Constitutional Alliance
Defending Dissent Foundation
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Fight for the Future
Golden Frog
Liberty Coalition
New America's Open Technology Institute
OpentheGovernment.org
PEN American Center
Silent Circle, LLC
Sunlight Foundation
World Privacy Forum

[12] 2ND PRIVACY ENGINEERING WORKSHOP, http://www.nist.gov/itl/csd/privacy-engineering-workshop-september-15-16-2014.cfm (last visited Nov. 14, 2014); see ALSO PRIVACY ENGINEERING WORKSHOP, http://www.nist.gov/itl/csd/privacy-engineering-workshop.cfm (last visited Nov. 14, 2014).