NIST Cryptographic Standards and Development Process

In the Matter of

NISTIR 7977 (NIST Standards and Development Process)

7 April 2014

Comments of the

Internet Architecture Board
c/o Internet Society
1775 Wiehle Avenue, Suite 201
Reston, VA 20190-5108
Website: http://www.iab.org
Email: iab@iab.org

NIST Cryptographic Standards and Development Process

In these comments, the Internet Architecture Board (IAB) responds to the comment period on NISTIR 7977, making recommendations relating to the review process for cybersecurity and cryptographic standards, in order to enhance transparency and openness.

Transparency and Accountability

The IAB appreciates the opportunity to comment on NIST's principles and practices afforded by the comment period on NISTIR 7977. NIST's focus on the principle of transparency is particularly welcome in light of the IAB's previous comments on SP 800-90 and our overall desire for transparency within the development of cryptographic standards.

The IAB wishes to call out in particular NIST's ongoing commitment to publish in the Federal Register the comments received on draft FIPS, as well as the dispositions of those comments. This provides both transparency and accountability, as it allows readers to understand the relationship between the comments received and the changes made. As the IAB made clear in its previous comments, this relationship is a key part of public trust in the development process.

We urge NIST to consider extending this publication of comments and dispositions to other NIST documents, including Recommendations and other Special Publications. While final publication might also be in the Federal Register, in order to provide continuity, the same information on a searchable portion of the NIST web site would serve the same purpose, as well as provide additional benefits. A searchable list of comments would enable NIST to provide a reply comment facility, something which is not possible with the current publication method. As noted in its previous comments, the IAB believes that a reply comment period and facility would improve not only transparency but the standards themselves, as it would give the research community and other interested technical individuals the opportunity to address issues which may have been raised to NIST.

The IAB also wishes to commend NIST on the work it does on early public outreach and for its involvement in cryptographic research. We note, however, that this involvement is necessarily limited by time and budget. Given those limitations, the IAB believes that it is vital to have the output of those outreach efforts brought into the externally visible part of the process. The externally visible process is where the broader community evaluates the developed standards, and that community needs to understand the impact of early review in order to comment and contribute further. In this light, we would like to re-iterate our previous recommendation that NIST provide a detailed and substantial explanation of changes resulting from internal review (even in cases where public comment was not initiated). This ensures that community evaluation proceeds from a more complete understanding of the inputs into the process.

In closing, thanks again for the opportunity to provide comments on the guidelines for the NIST Standards development process.