VCAT Subcommittee on Cybersecurity Report to the VCAT

July 14, 2014

The task

- In the 2013 Annual Report the VCAT made the following observation:

  “The VCAT values highly the ability of NIST to contribute independent technical expertise to international standards development processes for cryptography. In 2014, VCAT will lead an effort to validate NIST’s internal development processes”.
- The NIST Director charged the VCAT with forming a panel of experts in cryptography and security [a Committee of Visitors (CoV)] to assess NIST processes for the development of cryptographic standards.
- The VCAT Subcommittee on Cybersecurity was subsequently assigned the task of forming the CoV and preparing a report to the VCAT for deliberation.

The CoV

- The CoV was officially established in April comprising a distinguished panel of experts from academia, private sector, and standard development organizations. The members of the CoV are:
  - **Vint Cerf**, Vice President and Chief Evangelist, Google
  - **Edward Felten**, Director, Center for Information Technology Policy, Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University
  - **Steve Lipner**, Partner Director of Software Security, Microsoft Corporation
  - **Bart Preneel**, Professor Katholieke Universiteit Leuven, Belgium
  - **Ellen Richey**, Executive Vice President, Chief Enterprise Risk Officer and Chief Legal Officer, Visa Inc.
  - **Ron Rivest**, Vannevar Bush Professor, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology
  - **Fran Schrotter**, Senior Vice President and Chief Operating Officer, American National Standards Institute
- The CoV was given the following charge by the NIST Director Pat Gallager:

The Charge to the CoV

“In the area of cryptography, trust in the integrity of the National Institute of Standards and Technology (NIST) processes is critical to the agency’s ability to support international standards development efforts. Recently, concern has been expressed about one of the algorithms and the process that lead to its inclusion in Special Publication 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators* (January 2012 version). In November 2013, NIST initiated a review of its cryptographic standards development process in response to these concerns about the integrity of NIST cryptographic standards and guidelines.

As a critical component of this review, Dr. Patrick Gallagher has charged the NIST Visiting Committee on Advanced Technology (VCAT) to form a Committee of Visitors (COV) to serve as technical experts to assess NIST cryptographic standards and guidelines development process and if necessary provide findings on how it can be improved.

To assist the VCAT in this review, the VCAT has charged the COV to provide feedback on the ability of NIST to continue to assure the cryptographic community, users, and especially international partners of the technical soundness of NIST cryptographic reference materials and the validity of the process to update and amend these reference materials as needed. Specifically, the COV will:

- 1. Review NIST’s current cryptographic standards and guidelines development process and provide feedback on the principles that should drive these efforts, the processes for effectively engaging the cryptographic community and communicating with stakeholders, and NIST ability to fulfill its commitment to technical excellence.
- 2. Assess NIST cryptographic materials, noting when they adhere to or diverge from those principles and processes.

The COV members will deliver their individual assessments and findings to the VCAT Subcommittee on Cybersecurity for their consideration in the development of a final report to the VCAT and any subsequent recommendations given to NIST. “

Chronology

- The Subcommittee on Cybersecurity scheduled two teleconferences and one face-to-face meeting in the period of Apr 30 through May 29.
- NIST staff prepared, distributed, and presented a number of documents as documented in the Appendices of the report.
- Follow up sessions were scheduled between NIST staff and some members of the CoV in the first half of June.
- The CoV members delivered their individual reports to the Subcommittee between June 6 – June 20 and revised versions (only editorial changes) through July 7.
- The Subcommittee prepared, based on the CoV individual reports, the report submitted to the VCAT and officially approved it on July 7, 2014.

Next Step

- The VCAT endorses the Subcommittee on Cybersecurity Report and forwards it to the NIST Director as the VCAT final report.