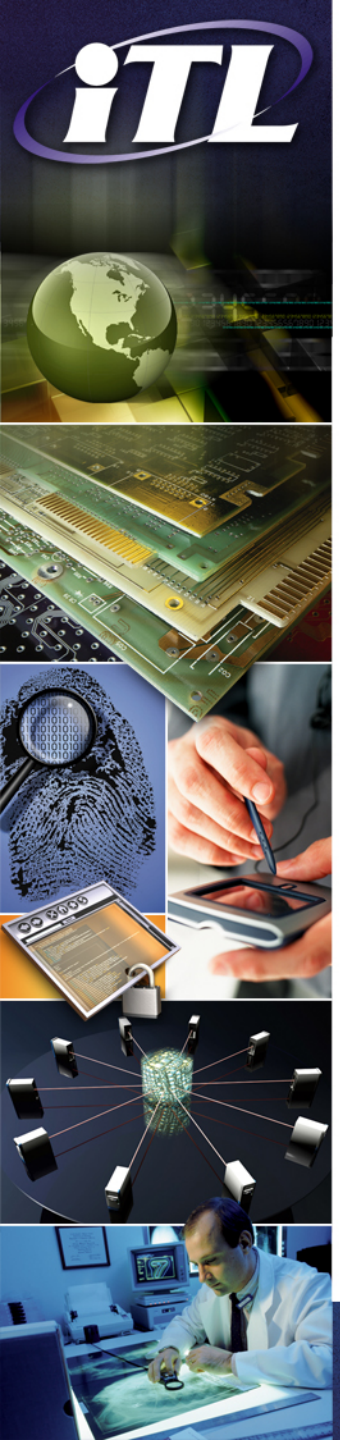


Cryptographic Standards Program Update

Andrew Regenscheid

October, 2014

Measurement Science for IT ◆ IT for Measurement Science

Summary of Events

- News Reports and Subsequent Concerns over Crypto Standards, September 2013
- Internal Discussion at NIST by NIST Staff and Leadership, Fall 2013
- NIST Publishes Draft IR 7977, Cryptographic Standards and Guidelines Development Process, February 2014
- NIST Director Sends Charge to VCAT to Review Cryptographic Activities, February 2014
- VCAT Subcommittee Forms Expert Committee of Visitors (COV), April 2014
- NIST Conducts Series of Briefings to VCAT Subcommittee and COV, May 2014
- COV Submits Individual Reports to VCAT Subcommittee, June 2014
- Full VCAT Provide Consensus Recommendation to NIST Director, July 2014.

Summary of VCAT Recommendations

- Openness and Transparency:
  - Develop and implement a plan to further increase the involvement of the cryptographic community, including academia and industry…
- Independent Strength/Capability:
  - Strive to increase the number of technical staff…
- Clarification of Relationship with NSA:
  - NIST may seek the advice of the NSA on cryptographic matters but it must be in a position to assess and reject it when warranted.
- Technical Work, Development and Processes:
  - NIST work openly with the cryptographic community to determine how best to address… the number of specific technical recommendations.

VCAT Recommendations

Openness and Transparency:

VCAT Recommendation

It is of paramount importance that NIST's process for developing cryptographic standards is open and transparent and has the trust and support of the cryptographic community. This includes improving the discipline required in carefully and openly documenting such developments.

NIST should also develop and implement a plan to further increase the involvement of the cryptographic community, including academia and industry, in the standards-development process.

The VCAT strongly encourages standards development through open competitions, where appropriate.

Courtesy Stoner Inc.

Courtesy Steuben

NIST Actions to Date

Openness and Transparency:

- NIST IR 7977, *NIST Cryptographic Standards and Guidelines Development Process*
- Public Posting of All Released Materials Requested Under FOIA
- Public Posting of COV Review Briefing Materials
- Open Discussions on Issue, VCAT Report and NIST Actions to Multiple Stakeholders for Awareness and Inputs.
  - *Examples Include:* IETF, ISO, ANSI, X9, IEEE, US Congressional Staff, US Industry, Industry Associations, Foreign Governments.

VCAT Recommendations

Independent Strength/Capability:

VCAT Recommendation

In order to be better positioned to exercise independent judgment on critical technical questions regarding cryptographic and security standards, NIST should strive to increase the number of technical staff with such expertise.

The VCAT also strongly suggests NIST explores, in addition to the current avenues, expanding its programs to engage academia and outside experts to aid in the review of specific technical topics.

Courtesy Stoner Inc.

Courtesy Steuben

NIST Actions to Date

Independent Strength/Capabilities:

- New Hire in Cryptographic Group (Daniel Smith-Tone)
- New Guest Researcher in Cryptographic Group (Meltem Turan)
- New Faculty Appointment in Cryptographic Group (Dr. Adam O'Neill, Georgetown)
- Washington DC-Area Cryptographic Group Meetings. Includes NIST, GWU, UMD, Georgetown)
- Establish and Strengthen the Pipeline of Staff and Engagements (MIT, KU Leuven)

VCAT Recommendations

Clarification of Relationship with NSA:

VCAT Recommendation

NIST may seek the advice of the NSA on cryptographic matters but it must be in a position to assess it and reject it when warranted. This may be accomplished by NIST itself or by engaging the cryptographic community during the development and review of any particular standard.

The VCAT recommends that NIST senior management reviews the current requirement for interaction with the NSA and requests changes where it hinders its ability to independently develop the best cryptographic standards to serve not only the United States Government but the broader community.

Courtesy Stoner Inc.

Courtesy Steuben

NIST Actions to Date

Clarification of Relationship with NSA

- All NSA contributions to NIST guidance will be acknowledged
- NIST – NSA Memo of Understanding (MOU) Publicly Posted
- Initial Introduction With New DIRNSA and NIST Director held
- Re-examination of the Current NIST – NSA MOU

VCAT Recommendations

Technical Work, Development and Processes:

VCAT Recommendation

The VCAT notes that the members of the CoV made a number of very specific technical recommendations. The VCAT recommends that NIST work openly with the cryptographic community to determine how best to address such recommendations.

The CoV reports also include a number of recommendations for improving the processes used in the development of cryptographic material. The VCAT recommends that NIST takes into account all such recommendations as it develops its guidelines and development process documents.

Courtesy Stoner Inc.

Courtesy Steuben

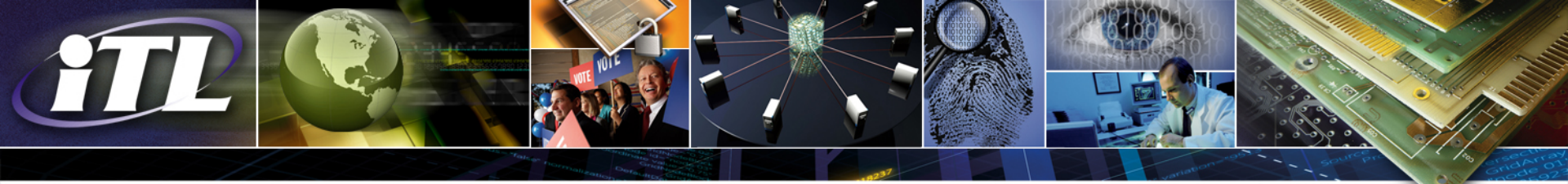
NIST Actions to Date

Technical Work, Development and Processes:

- Removal of Dual_EC_DRBG from Draft SP 800-90A
- Initiated Internal Review of NIST Cryptographic Reference Materials
- Participation With the IETF Cryptographic Forum Research Group
- Re-engineering the Configuration Management and Cryptographic Development Processes with NIST Standards Coordination Office
- Initial Draft Standard and Guideline IPR Review Process and IPR public query for new drafts completed with ITL Standards Coordinator

More Still Planned

- Six Federal Information Processing Standards (FIPS) Submitted for Consideration for Withdrawal
- Continue to Strengthen Capabilities with Hires; Guest Researchers; External Collaborations. Plan for Grants, Contracts and Engagements in the Next Fiscal Year
- Implement Process Improvements in Tools, Training and Institute Continual Review and Improvement Cycle
- Review and Improve Communication on Multiple Levels



Questions?

ISPAB, October, 2014