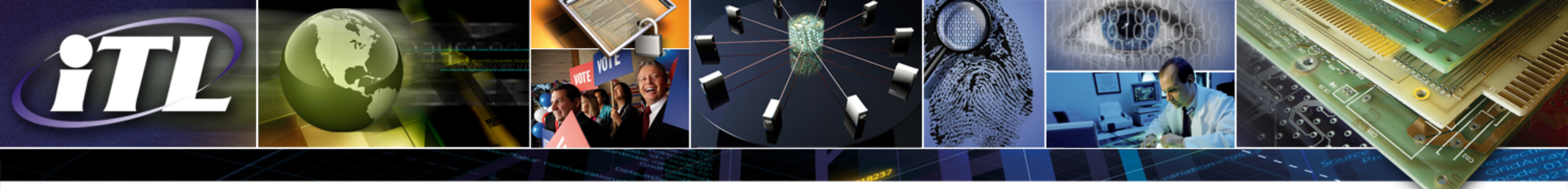
# NIST Cryptographic Standards Program

Charles H. Romine

October, 2014

*Measurement Science for IT ◆ IT for Measurement Science*

NIST
National Institute of Standards and Technology
U.S. Department of Commerce



# Summary of Events

- News reports of standards mistreatment by US Government
- Internal discussion at NIST by NIST staff and leadership, November 2013
- NIST publishes Draft NIST IR 7977, *Cryptographic Standards and Guidelines Development Process*, February 2014
- NIST Director sends charge to VCAT to review cryptographic activities, April 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 provides 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 in the development of NIST Standards
- Independent Strength/Capability:
  - strive to increase the number of NIST technical staff involved in cryptographic program
- 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.

# NIST Actions to Date

## ***Openness and Transparency:***

- NIST IR 7977, *NIST Cryptographic Standards and Guidelines Development Process* (DRAFT)
- Public posting of all released materials requested under FOIA
- Public posting of COV Review briefing materials
- Open discussions on the issue, the VCAT Report, and NIST actions, to multiple stakeholders for awareness and input
  - *Examples include:* IETF, ISO, ANSI, 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.

# NIST Actions to Date

## ***Independent Strength/Capabilities:***

- New hire in Cryptographic Technology Group (Daniel Smith-Tone)
- New guest researcher in Cryptographic Technology Group (Meltem Turan)
- New faculty appointment in Cryptographic Technology Group (Dr. Adam O'Neill, Georgetown)
- Creation of Washington DC-Area Cryptographic Group. Includes NIST, GWU, UMD, GMU, Georgetown)
- Strengthen the pipeline of staff and engagements (MIT, Katholieke Universiteit)

# 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.

# NIST Actions to Date

## *Clarification of Relationship with NSA*

- All NSA contributions to NIST guidance will be acknowledged
- NIST / NSA Memorandum of Understanding (MOU) publicly posted
- Initial introduction and discussion with new DIRNSA and NIST Director held
- Re-evaluation of the parameters of the current NIST / NSA MOU (in progress)

# 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.

# 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 input from the NIST Standards Coordination Office
- Initial Draft standard and guideline IPR review process and IPR public query for new drafts completed with ITL Standards Liaison

# More Still Planned

- Six Federal Information Processing Standards (FIPS) submitted for consideration for withdrawal

- Continue to strengthen capabilities with hires, guest researchers, external collaborations.  Planning for grants, contracts and engagements in FY2015 and beyond

- Implement process improvements in tools and training

- Institute continual review and improvement cycle

- Review and improve communication

# *The Information Technology Laboratory*

## *Questions?*

*VCAT October, 2014*