NIST Cryptographic Standards and Guidelines Development Process

Report and Recommendations of the
Visiting Committee on Advanced Technology
of the National Institute of Standards and Technology

July 2014

Preface

This report from Visiting Committee on Advanced Technology (VCAT) of the National Institute of Standards and Technology (NIST) to the NIST Director contains the VCAT's recommendations on how NIST can improve the cryptographic standards and guidelines development process.

The report is based on the report from the VCAT Subcommittee on Cybersecurity to the VCAT. The Subcommittee based its recommendations on inputs received from a distinguished panel of experts, the Committee of Visitors (CoV), that was established with the specific tasks of reviewing NIST cryptographic processes and of providing the Subcommittee their individual assessments.

The report is organized as follows. Section 1 contains a summary, in chronological order, of the events and meetings that occurred between February and June 2014 with detailed meeting minutes placed in appendices. Section 2 briefly discusses the individual CoV assessments and recommendations, with the original versions placed in appendices. Finally, Section 3 contains the VCAT observations and recommendations.

Table of Contents

1. Subcommittee on Cybersecurity and Committee of Visitors activities

At the Visiting Committee on Advanced Technology (VCAT) meeting that was held on February 4–5, 2014, NIST Director Dr. Patrick Gallagher tasked the VCAT with the establishment of a Committee of Visitors (CoV) to serve as technical experts in the review of National Institute of Standards and Technology (NIST) cryptographic standards and guidelines development process. This is an additional step in the overall review that NIST initiated in Nov 2013 of its cryptographic standards development process. The VCAT Subcommittee on Cybersecurity began the process of establishing the CoV and planning a series of teleconferences and meetings with the goal of having a preliminary set of individual observations and recommendations from the CoV members prior to the next scheduled VCAT meeting taking place on June 10–11.

The first task addressed by the Subcommittee was the formation of a panel of technical experts, namely the Committee of Visitors. With support provided by NIST staff, the CoV was successfully established by mid-April with a distinguished list of members from academia, the private sector, and standard development organizations. On behalf of the VCAT the Subcommittee expresses its deep appreciation to the CoV for their invaluable insight and the time and effort they devoted to this review. 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

On April 24th, NIST Director Dr. Patrick Gallagher issued a charge to the CoV (see Appendix A) outlining the tasks to be performed in assisting the VCAT Subcommittee with the review. The first teleconference took place on April 30th when the CoV was first introduced, the charge to

the CoV was reviewed in detail, and the beginning of the review process began. Appendix B contains the agenda and detailed meeting minutes and the list of documents that were made available for review.

A second teleconference took place on May 8th to continue the review process and also to discuss and finalize the agenda for the face-to-face meeting that was scheduled for the end of May. Appendix C contains the agenda and the detailed meeting minutes and the list of documents that were shared.

On May 29th, a full day, face-to-face meeting took place at NIST where most of the members were able to participate either in person or via webinar. Appendix D contains the agenda and the minutes of the meeting. The presentations from NIST staff gave first a historical perspective of NIST involvement in cryptographic standards, followed by a description of NIST statutory requirements, and a discussion of NIST interaction requirements with several federal agencies. A detailed presentation was made on the development of Special Publication (SP) 800-90 and in particular on the inclusion in the standard of the Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC DRBG) algorithm. The meeting concluded with presentations and discussions on the development of Special Series 800-38 standard and Federal Information Processing Standard (FIPS) 186, addressing block cipher modes and digital signatures, respectively.

The meeting concluded with all the participating members of the CoV committing to provide the VCAT Cybersecurity Subcommittee a preliminary individual assessment to aid in the development of the Subcommittee report to the VCAT. Since a member of the CoV could not participate at the May 29th meeting due to scheduling conflicts, a special session was held on June 11th for this member.

The VCAT met to consider and adopt the recommendations and finalize the report on July 14th, 2014.

2. CoV Individual Reports

The individual reports from the CoV were received by the Subcommittee between June 6th and June 20th and have been placed in Appendix E.

The review took place over a relatively short period of time but nonetheless the reports contain a large number of insightful comments and specific recommendations. Therefore, the VCAT felt it was in a position to complete a report and recommendations at this time.

3. Observations and Recommendations

The VCAT wants to take this opportunity to commend NIST, which during the course of this review has been forthcoming, open, and transparent, providing the CoV and Subcommittee with documentation when requested, answers to questions in a timely manner, and detailed presentations on a variety of subjects, including the development of SP 800-90 and in particular of the Dual EC DRBG.

The VCAT based on the material reviewed and in alignment with many CoV members' observations believes that the reconstruction of events was done in good faith and as thoroughly as possible, given the records and time available.

The CoV individual reports point out several shortcomings and procedural weaknesses that led to the inclusion of the Dual EC DRBG algorithm in SP 800-90 and propose several steps to remedy them. Therefore, the VCAT strongly urges NIST to consider the totality of recommendations from the CoV, and report back to the VCAT the overall NIST response.

In order to facilitate the formulation of a set of recommendations, as a synthesis of the CoV inputs, the VCAT identified four major categories that all CoV members addressed; such four categories are presented in the following subsections.

a. Openness and Transparency

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 standard development through open competitions, where appropriate.

b. Independent Strength and Capabilities

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.

c. Clarification of the Relationship with NSA

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.

d. Technical and other Issues

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.

Appendix A: Charge to the Committee of Visitors (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.

Appendix B: April 30, 2014 Kickoff Teleconference

Agenda

3:00 pm – 3:15 pm	**Welcome and Introduction of CoV Participants** Roberto Padovani, Chair, VCAT Subcommittee on Cybersecurity • Individual CoV members describe areas of expertise
3:15 pm – 3:45 pm	**Background-Public Concerns and Initial Steps by NIST** Donna Dodson, Chief Cybersecurity Advisory, Information and Technology Labortory (ITL) and Andy Regenscheid, Cryptographic Technology Group, ITL • Overview of NIST's current cryptographic standards and guidelines development process • Draft NIST IR 7977, *NIST Cryptographic Standards and Guidelines Development Process* and Public Comments Received
3:45 pm – 4:15 pm	**CoV Charge** Roberto Padovani, Chair, VCAT Subcommittee on Cybersecurity
4:15 pm – 4:45 pm	**Overview of CoV External Review Purpose, Scope, and Proposed Process and Timeline** Roberto Padovani, Chair, VCAT Subcommittee on Cybersecurity • Refine Process and Timeline, if needed • Public Engagement
4:45 pm – 5:00 pm	**Next Steps/Wrap Up** Roberto Padovani, Chair, VCAT Subcommittee on Cybersecurity • Identify initial areas of CoV focus/interest/concern

Meeting Summary

General Logistics and Procedures for the CoV

During this meeting, a number of procedural and scope items were clarified with the CoV. These included:

- **Communications**: The CoV requested that an email alias (cryptoCoV@nist.gov) be established. This alias will include: CoV members, VCAT Subcommittee members, Jason Boehm, Matt Scholl, Andy Regenscheid, Donna Dodson, Lily Chen, and Sara Caswell. You will be receiving separately information about your membership in that alias.
- **Development of a report**: Each CoV member is expected to develop an individual report describing their assessment and findings as outlined in the charge. These reports will serve as input to the VCAT Subcommittee on Cybersecurity, which will develop draft findings and recommendations for deliberation by the full VCAT committee. The full VCAT committee will then issue a formal report and recommendations. Due to federal FACA laws, the CoV members cannot generate a consensus report, but must issue individual findings.

- **Public engagement**: In the interest of transparency, NIST will issue a public announcement describing the work and membership of the CoV. NIST is still developing a plan for how and when to make documents and processes related to the CoV review public. NIST also plans to make the individual CoV reports public.
  If the public wishes to provide input to the review, they may do so in a number of ways:
    - CoV members may confer with and receive input from anyone they wish, and those conversations may influence the CoV members' reports and findings.
    - The VCAT meetings are open to the public, and time is set aside for the public to submit comments for the record during those meetings. The next VCAT meeting, when the progress of the CoV will be discussed, is on June 11, 2014.
- **Scope**: Some clarification of the scope of the CoV review is below:
    - The CoV is not expected to review every NIST cryptographic standard. NIST expects the CoV to "spot-check" specific standards relevant to their interests, and NIST will facilitate the decisions on which standards to review with a 1-3 page summary of each of NIST's standards.
    - The CoV should focus on the NIST process and materials; the processes of other organizations (eg, NSA, standards development organizations) are not in scope but can be used as reference or cited as examples if determined.
- **Timeline**: Beyond the timeline and process described in the "CoV External Review Purpose, Scope, and Proposed Process and Timeline", there are a few milestones to note. On June 10th, the VCAT Subcommittee on Cybersecurity will meet to review the CoV's findings to that date. On June 11th, the VCAT Subcommittee on Cybersecurity chair will report to the full VCAT the progress made by the CoV and Subcommittee to date. It is anticipated that the full work of the CoV won't yet be completed, and that those will be interim findings and progress reports. The VCAT meeting on June 11th is open to the public, and there will be time set aside for the public to enter their comments into the record.

Key Questions and Topics for Further Discussion

Through the meeting, CoV members asked a number of questions that highlighted their areas of focus, interest, and concern. NIST will work to generate briefing materials, deliver relevant documents, and make available subject matter experts (SMEs) who can help the CoV develop findings in those key areas. A summary of those question areas, and associated documents promised, is provided below.

Development of SP 800-90 and inclusion of Dual Elliptic Curve Random Bit Generator (Dual_EC_DRBG)

Since the primary issue driving this review is the inclusion of Dual_EC_DRBG in SP 800-90, the CoV asked that documents related to the development of Dual_EC_DRBG be made available for review. Due to the volume of material that could be included, NIST offered to provide summaries of the types of material that are available (eg, red-lined versions of SP 800-90, meeting notes, public comments, etc), and the CoV could choose to do a deeper dive in a given area. Since the exploration of this material will be an iterative process, the CoV asked that they be given a summary of the body of work as soon as possible. The CoV asked whether a formal internal investigation was conducted into the development of SP 800-90. While NIST did not conduct a formal investigation, it did a technical review and examined the

process of SP 800-90's development. NIST looks to the CoV to provide an independent review of NIST's crypto standards development processes – including those used for SP 800-90 – and expects the CoV's findings to contribute to VCAT recommendations in this area.

➔ NIST action item: generate and deliver to the CoV summary of document types related to the development of SP 800-90, as well as any documents related to NIST's internal reviews subsequent to the revelations in September 2013. NIST will work with NIST General Counsel and the CoV to make as many documents pertaining to the development of SP 800-90 available as possible.

NIST interactions with NSA

NIST's interactions with NSA are at the core of the public's concerns about NIST's cryptographic standards development process. As such, the CoV expressed desire to learn more about how NIST interacts with NSA in general, not just in the case of SP 800-90, and expected to generate findings related to those interactions.

➔ NIST action item: deliver to the CoV the Memorandum of Understanding between NIST and the NSA that formalizes roles and responsibilities
➔ NIST action item: work with NIST legal and the CoV to identify what other documents could be provided that would illustrate NIST/NSA interactions on cryptographic standards and guidelines

NIST cryptographic standards development process

While the CoV recognized that NISTIR 7977 was the first attempt to write down the NIST Cryptographic Standards Development Process, the CoV noted that they would likely require more detailed information to assess NIST's processes. The CoV also wanted to know more about the processes other standards-developing organizations use to benchmark NIST's processes against.

➔ NIST action item: send the CoV the Administrative Procedures Act for Rulemaking, which NIST follows for Federal Information Processing Standards (FIPS), though it is not legally required to.
➔ NIST action item: deliver the "Briefing Book," which will include 1-3 page descriptions of NIST's cryptographic standards materials, as well as the history of NIST's involvement in each area.

NIST cryptographic standards lifecycle

While NIST has started the process of describing its process for developing crypto standards, the CoV expressed interest in understanding more about the entire lifecycle of NIST's cryptographic standards. CoV members wanted to know how NIST decides to develop a standard in a specific area. NIST has heard both that they have too many and that they have too few standards. Some of these decisions are based on bandwidth, many are based on legislative scope. CoV members also noted the tension between cryptography as a discipline and the standards process, since cryptography is always advancing and algorithms can be broken. The high-level questions in this area included:

- How does NIST decide what cryptographic areas should be standardized?

- How does NIST choose what process (competition or otherwise) should be used to develop a standard?
- How does NIST review its standards to ensure they're still effective? How does NIST "retire" standards?
- How does the broader cryptographic standards-development ecosystem influence NIST's activities at each stage in the lifecycle?

➔ NIST action item: generate and deliver to the CoV briefing materials (eg, summaries, presentations, and availability of SMEs) relevant to the above questions.

➔ NIST action item: compile and deliver to the CoV the legislation that defines NIST's cryptographic responsibilities.

Attendees:

CoV Members

- **Edward Felten**, Director, Center for Information Technology Policy, and 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
- **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 (ANSI)
    - **Absent**
        - **Vint Cerf** Vice President and Chief Evangelist, Google

VCAT Subcommittee on Cybersecurity

- **Chair - Roberto Padovani**, Executive Vice President and Fellow, Qualcomm Technologies, Inc.
- **Rita Colwell**, Distinguished University Professor, University of Maryland, College Park and John Hopkins University Bloomberg School of Public Health; Senior Advisor and Chairman Emeritus, Canon U.S. Life Sciences
- **Al Romig**, Vice President, Advanced Development Programs Engineering and Advanced Systems, Lockheed Martin Aeronautics Company
    - **Absent**
        - **Bill Holt** Executive vice president and general manager of Intel Corporation's Technology and Manufacturing Group (TMG)

NIST Experts and Support Staff

Information Technology Laboratory (ITL)

- **Chuck Romine**, Director, ITL
- **Jim St. Pierre**, Deputy Director, ITL
- **Donna Dodson**, Chief Cybersecurity Advisor, ITL
- **Matt Scholl**, Acting Chief, Computer Security Division (CSD), ITL

- **Lily Chen**, Acting Manager, Cryptographic Technology Group, CSD, ITL
- **Andy Regenscheid**, Cryptographic Technology Group, CSD, ITL
- **Sara Caswell**, Cryptographic Technology Group, CSD, ITL

NIST Director's Office

- **Jason Boehm**, Director, Program Coordination Office
- **Gail Ehrlich**, VCAT Executive Director
- **Laurel Miner**, Analyst
- **Bill Newhouse**, Analyst

Documents Provided:

- Agenda for April 30 CoV Kickoff Meeting
- List of CoV, VCAT Subcommittee on Cybersecurity, and NIST Participants
- CoV Charge
- CoV External Review Purpose, Scope, and Proposed Process and Timeline
- Draft NISTIR 7977, *NIST Cryptographic Standards and Guidelines Development Process*
- Comments Received on Draft NISTIR 7977
- NIST Briefing Slides: Background-Public Concerns and Initial Steps

Appendix C: May 8, 2014 Teleconference

Agenda

4:00 pm – 4:10 pm	**Welcome** Roberto Padovani, Chair, VCAT Subcommittee on Cybersecurity
4:10 pm – 4:20 pm	**Briefing Book Overview** Andrew Regenscheid, Cryptographic Technology Group, NIST
4:20 pm – 4:30 pm	**CoV Face-to-Face Meeting Planning** Roberto Padovani, Chair, VCAT Subcommittee on Cybersecurity • Meeting logistics • Review draft agenda
4:30 pm – 4:55 pm	**CoV Members Priorities** Roberto Padovani, Chair, VCAT Subcommittee on Cybersecurity • CoV members can prioritize what they would like to have available at the face-to-face meeting (i.e., presentation on a specific topic, specific write-up, set of documents)
4:55 pm – 5:00 pm	**Questions and Wrap Up**

Meeting Summary

Updates from NIST

The meeting started with some updates based on topics discussed during the kickoff meeting.

- **Availability of materials currently under FOIA related to past cryptographic development efforts**: After consulting the NIST FOIA official and NIST General Counsel, NIST noted the following:
    - NIST will be as open as possible with materials currently under FOIA. NIST will discuss and describe any and all FOIA-related materials that the CoV and Subcommittee would like to explore. NIST can describe the substance or essence of cryptographic development process communications between NIST and outside parties to the CoV.
    - NIST will share source material with the CoV as soon as it has been reviewed and cleared for release in response to a current FOIA request.
        - NIST's internal communications are being cleared as quickly as possible, and NIST hopes to have those materials available to share with the CoV soon.
        - NIST's communications with NSA are being reviewed by NSA, a process which is out of NIST's control. NIST has asked NSA to expedite their review.
    - Since the VCAT Subcommittee on Cybersecurity members are special government employees, NIST can share with them source documents of any material related to cryptographic standards development.

- **Public Announcement of CoV Membership:** The members will receive a draft of the public announcement. NIST released the public announcement on May 14 and is available at: http://www.nist.gov/director/vcat/vcat-051414.cfm

Briefing Book Overview and related discussion on review scope

- NIST described the **contents of the Briefing Book** that was to be delivered on May 13 to the CoV members.
    - The Briefing Book includes 1-2 page summaries of five Federal Information Processing Standards and nineteen 800 Series Special Publications. These summaries are intended to help the CoV members narrow and prioritize the portfolio of NIST cryptographic publications for further analysis. These summaries include:
        - Scope
        - Purpose/identified need
        - Contributors
        - Timeline
        - Public Engagement
        - Major decision(s)

- This review prompted a discussion on the scope of the review. In summary, the Briefing Book represents a selection of NIST's cryptographic standard portfolio. The documents in the Briefing Book are not meant to define the scope of the CoV's investigation. These documents were chosen because NIST thought they would be the most relevant to the CoV's inquiries.
    - However, this selection is not intended to limit the CoV's investigation; the CoV may ask for deeper dives on any of NIST's cryptographic standards, including those not covered in the Briefing Book.
    - NIST also does not expect the CoV to investigate all 24 of the documents summarized in the Briefing Book. The CoV is free to choose its own selection of documents from that portfolio.
    - NIST is reluctant to suggest a narrower set of publications for the CoV to review. If the CoV wants to suggest a decision rule or common criteria (eg, "those publications with significant NSA involvement"), NIST can help them choose those publications.
    - The CoV members raised the point that if they do not provide recommendations on a particular publication, it might imply that the members approve the technical merit of process behind that publication. The CoV agreed that disclaimers against that assumption would be useful front-matter for the individual reports.

Other items discussed:

- The draft agenda for the May 29th meeting was reviewed. The CoV noted that after review of the Briefing Book, the agenda for the meeting could be revised via email. The CoV asked whether anyone from NSA would attend the May 29th meeting; NIST said there were no plans for that yet but that they would look into the possibility. NIST contacted NSA and no one from NSA will be attending this meeting.
- Fran Schrotter asked that the ANSI X9 be referred to by its proper title: the " Accredited Standards Committee X9" or simply X9.
- On the topic of choosing what cryptographic item should be standardized, a suggestion was made that NIST could consider focusing on crypto APIs. NIST acknowledged that it has not been

very active in this area, and that the CoV may want to include this consideration in its analysis of how NIST chooses standardization areas.

- There is no template or recommended focus for the individual CoV members' reports and findings. If a CoV member wanted a template, NIST could prepare a suggested outline or identify specific topics.

Attendees:

CoV Members

- **Edward Felten**, Director, Center for Information Technology Policy, and Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University
- **Bart Preneel**, Professor, Katholieke Universiteit Leuven
- **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 (ANSI)
    - **Absent**
        - **Vint Cerf**, Vice President and Chief Evangelist, Google
        - **Steve Lipner**, Partner Director of Software Security Microsoft Corporation
        - **Ellen Richey**, Executive Vice President, Chief Enterprise Risk Officer, and Chief Legal Officer, Visa Inc.

VCAT Subcommittee on Cybersecurity

- **Chair - Roberto Padovani**, Executive Vice President and Fellow, Qualcomm Technologies, Inc.
- **Rita Colwell**, Distinguished University Professor, University of Maryland, College Park and John Hopkins University Bloomberg School of Public Health; Senior Advisor and Chairman Emeritus, Canon U.S. Life Sciences
- **Al Romig**, Vice President, Advanced Development Programs Engineering and Advanced Systems, Lockheed Martin Aeronautics Company
    - **Absent:**
        - **Bill Holt,** Executive vice president and general manager of Intel Corporation's Technology and Manufacturing Group (TMG)

NIST Experts and Support Staff

Information Technology Laboratory (ITL)

- **Chuck Romine**, Director, ITL
- **Jim St. Pierre**, Deputy Director, ITL
- **Matt Scholl**, Acting Chief, Computer Security Division (CSD), ITL
- **Lily Chen**, Acting Manager, Cryptographic Technology Group, CSD, ITL
- **Andy Regenscheid**, Cryptographic Technology Group, CSD, ITL

NIST Director's Office

- **Jason Boehm**, Director, Program Coordination Office
- **Gail Ehrlich**, VCAT Executive Director

- **Laurel Miner**, Analyst
- **Bill Newhouse**, Analyst (ITL)

Documents Provided:

- Agenda for May 8 CoV Telecon
- 2010 NIST NSA Memorandum of Understanding (MOU)
- 1989 NIST NSA MOU
- Proposed Agenda for May 29 Face-to-Face CoV Meeting
- Administrative Procedure Act for Rulemaking

Appendix D: May 29, 2014 Face-to-Face Meeting

Agenda

8:00 am – 8:15 am	**Review Purpose and Agenda** Roberto Padovani, Chair, VCAT Subcommittee on Cybersecurity
8:15 am – 9:45 am	**Discussion of NIST Cryptographic Standards & Guidelines Development Process** Donna Dodson, Chief Cybersecurity Advisor, NIST Andrew Regenscheid, Cryptographic Technology Group, NIST • Overview of mission and statutory authority/responsibilities • Engagements with external organizations • Discussion with CoV
9:45 am – 10:00 am	**Break**
10:00 am – 11:30 am	**Discussion of Specific NIST Cryptographic Standards & Guidelines Publications** • Dual EC in X9.82 and SP 800-90 *John Kelsey and Elaine Barker, NIST*
11:30 am – 12:30 pm	**Lunch**
12:30 pm – 1:45 pm	**Discussion of Specific NIST Cryptographic Standards & Guidelines Publications** (con't) • Development of SP 800-38 Series for Block Cipher Modes *Morris Dworkin, NIST* • Development of FIPS 186: Digital Signatures (and Elliptic Curves) *Dustin Moody, NIST*
1:45 pm – 2:00 pm	**Break**
2:00 pm – 3:00 pm	**Open Discussion and Interim Individual Assessments and Findings** Roberto Padovani, Chair, VCAT Subcommittee on Cybersecurity

Meeting Summary

Review Purpose and Agenda

Roberto Padovani, Chair for the VCAT Subcommittee on Cybersecurity, reviewed the charge for the CoV, which is to:

- 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.

- Assess NIST cryptographic materials, noting when they adhere to or diverge from those principles and processes.

Padovani reminded CoV members that they 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 to NIST.

Discussion of NIST Cryptographic Standards & Guidelines Development Process

Donna Dodson and Andrew Regenscheid reviewed NIST's Cryptographic Standards & Guidelines Development Process. This involved a lengthy discussion of the history of NIST/NBS's work in cryptographic standards, the statutory authorities NIST has, and the mechanisms for developing and promulgating NIST's standards and guidelines among federal agencies.

Key discussion points:

- NIST has a long history in developing cryptographic standards and guidelines. Though NIST standards are directed at non-classified federal information technology systems, NIST notes that a much broader community, including private industry and international organizations, use them.
- NIST has a testing program for several of its cryptographic standards and guidelines. In 1995, NIST established the Cryptographic Module Validation Program[1] (CMVP) that validates cryptographic modules to Federal Information Processing Standards Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards and guidelines.
- NIST works closely with Federal agencies (including the civilian agencies, NSA, DHS, the Committee for National Security Systems (CNSS), and the Office of Management and Budget) industry, and academia on the development of its cybersecurity standards and guidelines including those in cryptography.
- NIST provided an example of it works with the DoD in cybersecurity. The DoD has declared that the cybersecurity requirements for DOD information technologies will be managed through the Risk Management Framework (RMF) consistent with the principles established in NIST SP-800-37. NIST provided the relevant DoD instructions to the CoV.
- NSA specifies a subset of NIST cryptographic algorithms through the NSA Suite B program. NSA's Information Assurance Directorate recognizes these algorithms in solutions approved for protecting National Security Systems. NIST sent the link[2] to NSA's website for more details on these algorithms.
- NIST's coordination with the NSA on cryptographic standards is currently required by legislation [*Federal Information Security Management Act of 2002*]. There is an amendment offered by Rep. Grayson on NIST's authorizing legislation to remove that requirement, and NIST has issued a response to this amendment. NIST circulated all relevant legislation, Rep. Grayson's letter to Pat Gallagher and NIST's response to Rep. Grayson to the CoV.

[1] http://csrc.nist.gov/groups/STM/cmvp/
[2] http://www.nsa.gov/ia/programs/suiteb_cryptography/

- There were a number of questions about the NIST/NSA Memorandum of Understanding and the extent of NSA's influence on NIST's cryptographic standards. NIST acknowledged that not all of NSA's feedback on draft standards is a part of the public record. NSA's involvement is most often acknowledged as a contribution in the front matter in the standard. However, specific contributors are not always acknowledged due to time constraints with clearance through NSA's pre-publication review process. NIST expressed that this is changing – NIST is now requiring that all of NSA's contributions and authorship will be acknowledged in the relevant standard.
- There was some discussion about the process for responding to private, anonymous, and/or informal comments on draft standards. The need for balance between promoting widespread comment and ensuring transparency was identified. It was also noted that once a cryptographic standard is in place, those standards have significant reach and lifetime. Even once NIST retracts/sunsets a standard, they find that it can remain in systems for a significant period of time.

Discussion of Specific NIST Cryptographic Standards & Guidelines Publications

DUAL EC IN X9.82 AND SP 800-90

John Kelsey presented a detailed history on the development of the Dual Elliptic Curve Deterministic Random Bit Generator (Dual_EC_DRBG) in American National Standard X9.82 Part 3 and NIST Special Publication 800-90A. The presentation described NIST's work within ASC X9 on X9.82 and NIST's decision develop to a Special Publication based on the contributions to X9. The presentation described how Dual_EC DRBG was incorporated into these two documents, and how early concerns with the security of this algorithm were initially addressed in the two publications. NIST acknowledged that these concerns, which came up during the standards development process within X9, should have led to more substantial changes to the documents, and identified several deficiencies in the steps that were taken. The CoV asked a number of clarifying questions, and more nuances to this standard were revealed.

***Key discussion points*:**

- NIST staff and the CoV discussed the long, complicated processes that were used to develop ANS X9.82 and NIST SP 800-90A, whose development overlapped. NIST collaborated with the NSA on these documents, both within X9 and on the NIST Special Publication.
- NIST provided the editor for ANS X9.82 Part 3 when the project began in 1998. As editor, it was NIST's role to include contributions from X9 members as directed by the group.
- As members of the X9.82 development committee, NIST contributed two DRBG designs based on symmetric cryptography (i.e., HMAC_DRBG and CTR_DRBG) and provided substantial comments to HASH_DRBG. NSA contributed Dual_EC_DRBG and HASH_DRBG.
- NIST focused its efforts on the algorithms it contributed and the other algorithms based on symmetric cryptography, areas of expertise for the NIST participants.
- In the standards development process, cryptographers identified two security issues with Dual_EC_DRBG: 1) the possibility of a backdoor in the algorithm based on the specific parameters, and 2) a statistical bias in the output of the DRBG (e.g., like a weighted die).
- The CoV members asked NIST to clarify that the bias issue and the potential backdoor in the parameters are not explicitly related, though removing the bias would have made it impractical to exploit the potential backdoor.

- Comments on the potential backdoor led X9 and NIST to include a method for generating alternative parameters in X9.82 Part 3 and NIST SP 800-90A. However, the original parameters were recommended for use, and were required to be included by implementations seeking validation under NIST's Cryptographic Module Validation Program (CMVP).
- NIST explained that it did not make more changes to the Dual_EC_DRBG specification because the DoD was already using the algorithm as originally specified, and NIST believed a backdoor in the algorithm was unlikely.
- When evaluating Dual_EC_DRBG, NIST asked itself "Do we think there is a trapdoor?" when it should have asked, "Should we include an algorithm in our standards that could have a trapdoor?"
- The CoV asked where Dual_EC_DRBG was used. NIST said over 50 cryptographic modules validated by CMVP implemented Dual_EC_DRBG, but explained that does not mean the algorithm was widely used by security products. The group noted that some versions of the RSA BSAFE[3] cryptography library implemented Dual_EC_DRBG by default.
- The CoV discussed patents issues associated with Dual_EC_DRBG. This included patents on elliptic curve cryptography techniques that underpin Dual_EC_(held by Certicom and licensed to NSA[4]), and patents related to the generation of alternative parameters for Dual_EC_DRBG.

Development of SP 800-38 Series for Block Cipher Modes

Morris Dworkin presented an overview of NIST's recommendations on block cipher modes of operation. A block cipher mode of operation (or just a "mode") is a specified method for using a block cipher primitive to achieve some security protection such as data confidentiality (or encryption) or authentication (including integrity). The presentation described the process NIST uses to vet proposed modes of operation and provided an overview of the modes included in the NIST toolkit. It also described NIST's consultation with NSA, and a summary of the difficult decisions NIST made in the modes project. The role of security proofs, the effects of patents, the availability of free copies of standards for review and analysis and the fast pace of NIST mode standard adoption elicited significant discussion.

***Key discussion points*:**

- NIST has largely set the accepted standards for block cipher modes of operation since 1980, but, after the adoption of the Advanced Encryption Standard, NIST initiated an open call for the public to submit new proposed mode standards to NIST. NIST now has six SP 800-38 series publications that specify 14 different encryption, authentication and AEAD modes.
- A mode of operation proof sets mode security bounds and proves that violating those bounds reduces to breaking the block cipher used. However, the NSA designed Key Wrap mode (SP 800-38F), while apparently very secure, has no proof. The CoV discussed mode proofs and members asked: without a proof, why should NIST adopt a mode standard, and how would NIST evaluate the security?

[3] https://www.emc.com/security/rsa-bsafe.htm
[4] http://www.nsa.gov/business/programs/quick_facts.shtml

- Patents are a factor in modes standards. NIST adopted GCM, an efficient AEAD mode, largely because of a difficult patent situation with other, probably more robust and even more efficient submissions.
- The CoV discussed the merits of freely-available cryptographic standards. In particular, the XTS mode approved in NIST SP 800-38E references IEEE Std. 1619-2007 instead of providing the specification. While a version of IEEE Std. 1619-2007 was freely-available during the public comment period on SP 800-38E, implementers and researchers would now need to pay for this standard.
- NIST provided the CoV OMB circular A-119, Revised (1997), which describes federal government policies on the development and use of voluntary consensus standards and in conformity assessment activities
- CoV members discussed whether NIST has adopted too many new modes too rapidly: are they all needed and, in particular, is it appropriate to adopt modes such as XTS that cater to narrow industry needs? Should NIST do fewer mode standards and take more time to permit better analysis?

Development of FIPS 186: Digital Signatures (and Elliptic Curves)

Dustin Moody gave an overview of the NIST Digital Signature Standard, FIPS 186, and the development of the "NIST Curves," a set of 15 recommended elliptic curves generated by NSA, used for elliptic curve digital signatures and key agreement. He also discussed concerns about the provenance and security of the NIST curves and whether they might have hidden weaknesses and concluded that there are no known attacks that weaken the claimed security of the NIST curves.

***Key discussion points*:**

- The NIST toolkit includes two types of curves- pseudorandom curves and special curves.
- There was a discussion of potential security concerns with how the NIST pseudorandom curves were generated. The NIST curves were generated from a seed using a one-way function (SHA-1), following an algorithm described in ANS X9.62. NIST has verified that this is how the parameters were generated.
- NIST and the CoV discussed the concern that these curves could have a hidden weakness, if the NSA knew of some weakness unknown to the academic community and was able to try a large number of seeds until finding a curve with such a weakness. While NIST could not say how many seeds were attempted during the generation process, the presenter noted that the research community is still not aware of any sufficiently large class of weak curves to make this practical.
- Much of the NIST work and discussion of Digital Signature Standards and elliptic curves involved the X9 standards committee and FIPS 186 makes normative references to X9.31 and X9.62. The merits of free availability of consensus standards, to enable broad early review, was discussed. OMB circular A-119, Revised (1997), sets policies for the federal government for consensus standards and conformity assessment. NIST sent this circular to the CoV members.
- Some discussion centered on around why NIST standardized curves that create attack targets. The answer: NIST created recommended curves to facilitate interoperability and to give users well-vetted choices.

- New curves with better performance or security proprieties such as side-channel resistance) have been developed since the 1990s-era NIST curves. It may be time to consider adding additional recommended curves, developed in a more public process and with some arguably better properties.

Attendees (* indicates attended remotely via webinar):

CoV Members

- **Vint Cerf**, Vice President and Chief Evangelist, Google
- **Edward Felten**, Director, Center for Information Technology Policy, and 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
- **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 (ANSI)
    - **Absent**
        - **Ellen Richey**, Executive Vice President, Chief Enterprise Risk Officer, and Chief Legal Officer, Visa Inc.

VCAT Subcommittee on Cybersecurity

- **Chair - Roberto Padovani***, Executive Vice President and Fellow, Qualcomm Technologies, Inc.
- **Rita Colwell**, Distinguished University Professor, University of Maryland, College Park and John Hopkins University Bloomberg School of Public Health; Senior Advisor and Chairman Emeritus, Canon U.S. Life Sciences
    - **Absent:**
        - **Bill Holt,** Executive vice president and general manager of Intel Corporation's Technology and Manufacturing Group (TMG)
        - **Al Romig**, Vice President, Advanced Development Programs Engineering and Advanced Systems, Lockheed Martin Aeronautics Company

NIST Experts and Support Staff

Information Technology Laboratory (ITL)

- **Chuck Romine**, Director, ITL
- **Jim St. Pierre**, Deputy Director, ITL
- **Matt Scholl**, Acting Chief, Computer Security Division (CSD), ITL
- **Lily Chen**, Acting Manager, Cryptographic Technology Group, CSD, ITL
- **Elaine Barker**, Cryptographic Technology Group, CSD, ITL
- **Bill Burr**, Cryptographic Technology Group, CSD, ITL
- **Morris Dworkin**, Cryptographic Technology Group, CSD, ITL
- **John Kelsey**, Cryptographic Technology Group, CSD, ITL
- **Dustin Moody**, Cryptographic Technology Group, CSD, ITL
- **Andy Regenscheid**, Cryptographic Technology Group, CSD, ITL

NIST Director's Office

- **Willie E. May**, Associate Director for Laboratory Programs
- **Jason Boehm**, Director, Program Coordination Office
- **Gail Ehrlich**, VCAT Executive Director
- **Laurel Miner**, Analyst
- **Bill Newhouse**, Analyst (ITL)

Documents Provided:

- Final Agenda for May 29
- Computer Security Act of 1987
- Federal Information Security Management Act of 2002
- Letter from Rep. Grayson and Response from NIST Director Gallagher
- OMB Circular A-119
- Powerpoint presentations for Discussion of Specific NIST Cryptographic Standards & Guidelines Publications

Appendix E: Committee of Visitors Individual Reports

Date: 6 June 2014

To: Roberto Padovani, Chairman

From: Vinton Cerf, VP Google

Subject: COMMITTEE OF VISITORS (COV) ON THE CRYPTOGRAPHIC AND SECURITY PROGRAM AT NIST

The COV met at NIST on May 29, 2014. NIST representatives reviewed the history of NIST's work in cryptographic standards, including an in-depth and extremely candid assessment of NIST's involvement in the Digital Equipment Standard, the Suite B Dual EC Deterministic Random Bit Generator (Dual EC DRBG), the Advanced Encryption Standard and security guideline publications (FISMA publications).

NIST is to be commended for its candid and transparent self-review of the procedures undertaken to reach adoption of specific cryptographic standards. The COV was given completely open access to any documentation requested and this includes FOIA information that the COV did not request but which was delivered voluntarily by NIST to the COV.

In my opinion, NIST representatives were particularly and probably overly hard on themselves in analyzing the Dual EC DRBG matter, but the retrospective analysis reinforces my view that NIST must achieve sufficient depth of cryptographic and mathematical knowledge to render itself fully capable of evaluating strength and weakness of proposed algorithms without dependence on NSA. This almost certainly means hiring more cryptographers and mathematicians with well-respected and well-earned reputations.

Specific recommendations:

1. NIST must retain and reinforce an extremely open, documented and transparent process for the development or revision of standards for security, especially the process by which cryptographic standards are developed. The AES development is a prime example of such an open and transparent process.
2. NIST cannot be seen as nor be subject to any kind of coercion or veto by the National Security Agency. Transparency of process will help here but this also means that NIST must have credible independent depth in cryptographic and mathematical staff.
3. Given the questionable utility of the NSA-recommended Dual EC DRBG algorithm and the potential for "backdoor" selection of the P,Q parameters, NIST is justified in removing this algorithm from its recommendations.
4. FIPS186-4 contains, in Appendix A, guidelines for the selection of elliptic curve parameters. It appears to me that this text satisfies Rivest's

recommendation 6, to wit, that guidance should be provided to allow users of ECDSA to generate their own parameters for the selection of elliptic curves.

5. To the extent that patent licenses are required from Research in Motion, now the owner of Certicom, for the use of elliptic curve cryptography, it may prove appropriate to assure that the NIST standards can be practiced freely by any adopters. This may require acquisition by NIST of patent licenses independent of those already obtained by NSA.
6. Reiterating Rivest: do not use the term “random” where “pseudo-random” is, in fact, the proper way to describe the output of an algorithm or method.

While it is beyond the remit of this committee to opine on the mission and practices of the National Security Agency, it cannot be accepted that NIST’s responsibilities should be co-opted by the NSA’s intelligence mission. NIST’s responsibility is to identify means of protecting information to the maximum practicable extent and this must be its primary metric and objective.

Assessment of NIST Cryptographic Standards and Process

Edward W. Felten
Princeton University

June 6, 2014

Introduction

Disclosures by Edward Snowden and others have called into question the security of certain NIST cryptographic standards and the integrity of NIST's standard-making processes. As part of NIST's response to these concerns, NIST Director Patrick Gallagher asked NIST's Visiting Committee on Advanced Technology (VCAT) to appoint a Committee of Visitors (CoV) to assess NIST's cryptographic standards and processes and make recommendations. I am one of the seven members of the CoV. Individual members of the CoV were asked to submit separate assessments to VCAT. This is my assessment.

The specific charge to the CoV was:

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 held several telephone meetings and a one-day face-to-face meeting at NIST. The CoV received materials and briefings from NIST and met with NIST personnel. NIST was very helpful and forthcoming in these briefings and meetings.

I understand that there are some relevant documents that cannot yet be released to the CoV because the documents are undergoing a necessary legal review. I will revise this assessment if necessary after those documents become available for review.

Role and Importance of NIST Cryptographic Standards[1]

In addition to its role in creating cryptographic standards that are used within the U.S. government, NIST has played an important role in supporting cryptographic standards and security more generally. NIST convenes discussions of existing and proposed cryptographic standards, and helps to coordinate collective efforts across the cryptographic community of the type that lead to the most secure standards. Collaboration between NIST and the cryptographic community has led to some of the longest-lasting and most trusted cryptographic standards, and

[1] For brevity, I will use the term "standards" to refer to NIST publications that are formally captioned as "standards" as well as those that are captioned as "special publications" or "guidelines".

many in the cryptographic community have considered NIST's cryptographic recommendations to be the "gold standard."

NIST standards provide the greatest benefits to the American people, American industry, and the U.S. government when those standards are adopted widely. If users have confidence in NIST standards, technology vendors are more likely to adopt NIST standards, thereby ensuring that U.S. government agencies, which are required to follow NIST standards, will be able to adopt the most popular technologies and products. A bifurcated world in which the U.S. government uses NIST standards and everyone else uses different standards would be worse for everybody and would prevent government agencies from using Commercial Off-the-Shelf technologies and frustrate interoperation between government and non-government systems.

Widespread adoption of NIST standards depends on widespread confidence that NIST standards are of the highest quality, and especially on confidence that NIST standards are as secure as possible and do not allow trapdoor access by the U.S. government or anyone else.

Recommendation: *NIST should reiterate clearly the importance of fostering widespread justified confidence in NIST's cryptographic standards and recommendations. Widespread confidence advances NIST's goals, enabling better security for all users of NIST standards.*

NIST and NSA

NIST is required by statute to consult with the National Security Agency (NSA) in its standards development work.[2] NSA has enormous expertise in cryptography and has the capability to provide advice to NIST that strengthens standards. NSA has provided such helpful advice in the past. For example, NSA suggested enhancements to the Data Encryption Standard (improving the DES "S-boxes")[3] and the Secure Hash Algorithm (improving the original algorithm, known as SHA-0, to create a better algorithm, SHA-1).

At the same time, a primary mission of NSA is Signals Intelligence (SIGINT) which involves intercepting and decoding communications. NSA's SIGINT mission can benefit from weaknesses in standards, especially if those weaknesses are not widely known outside NSA. Because of this, NSA has an undeniable incentive to influence standards in ways that allow NSA to defeat the standards' security. Documents disclosed by Edward Snowden confirm that NSA has (or had recently) an active "SIGINT Enabling" program to "[i]nsert vulnerabilities into

[2] See, e.g., 44 U.S.C. 35.3543(a)(3).

[3] NSA also played a role in the decision to reduce the key size in DES from the initially proposed 64 bits, to 56 bits, a decision about which NIST should have been skeptical. NIST does not presently have a written record of the process back in the 1970s that led to the decision to reduce the DES key size to 56 bits. The reduction in key size reduced the security of DES and hastened the eventual demise of DES. Based on the available evidence, I am not aware of a technical justification for reducing the key size to 56 bits. For example, the 56-bit version of DES is no faster than a 64-bit version would have been. The key size reduction in DES, which was advocated by NSA, may be an early indication of NSA's mixed motives regarding cryptographic standards.

commercial encryption systems" and "[i]nfluence policies, standards, and specification for commercial public key technologies."[4] "These design changes make the systems in question exploitable through SIGINT collection .... To the consumer and other adversaries, however, the systems' security remains intact." In other words, NSA has had a program whose goals include creating weaknesses in products and standards.

Recommendation: *Because of NSA's SIGINT mission, NIST should be very careful in its interactions with NSA regarding standards. NIST should draw on NSA's expertise, but NIST must not defer to NSA on security-relevant decisions. NIST itself, and the cryptographic community that looks to NIST's standards, must be able to conclude confidently that NSA did not have any opportunity to undermine any NIST standard.*

The relationship between NIST and NSA is guided by a Memorandum of Understanding, written in 1989 and revised in 2010, which creates a Technical Working Group (TWG) whose members are chosen equally by both agencies, and defines practices for the operation of the TWG. The 1989 version of the MOU stated[5] that

> The NIST and the NSA shall ...
> Ensure the Technical Working Group reviews prior to public disclosure all matters regarding technical systems security techniques to be developed for use in protecting sensitive information in federal computer systems to ensure they are consistent with the national security of the United States. If NIST and NSA are unable to resolve such an issue within 60 days, either agency may elect to raise the issue to the Secretary of Defense and the Secretary of Commerce. It is recognized that such an issue may be referred to the President through the [National Security Council] for resolution. No action shall be taken on such an issue until it is resolved.

The 2010 version of the MOU, which superseded the earlier version, stated[6] that

> The NIST and the NSA shall ...
> Ensure the Technical Working Group reviews, prior to public disclosure, all matters regarding technical systems security techniques to be developed for use in protecting non-national security systems and the information that resides therein, to ensure they are consistent with the national security of the United States.

To the extent that the 1989 version may have been interpreted as giving NSA an effective veto over the content of NIST standards, such a veto would have been inappropriate and possibly inconsistent with statute. The 2010 version of the MOU appears to be more consistent with the statutory requirement that NIST consult with NSA before NIST issues standards.

---

[4] Document leaked by Edward Snowden, captioned as "Computer Network Operations SIGINT Enabling".
[5] 1989 NIST/NSA MOU, pages 3-4, paragraph 7.
[6] 2010 NIST/NSA MOU, pages 3-4, paragraph 5.

Recommendation: *NIST should review its Memorandum of Understanding with NSA to make sure that the MOU is consistent with the standard-making autonomy granted to NIST by statute.*

On Cryptographic Trapdoors

The main concerns raised about NIST cryptographic standards relate to the possibility that NSA might have a trapdoor to certain standards. When a party has a trapdoor to a standard, this means that the party has some knowledge not available to the public that gives the party a secret ability to defeat the standard's security guarantee.

It is sometimes argued that an NSA trapdoor can benefit the United States on balance, as long as it is a "pure trapdoor," in the sense that NSA is the only party who can possibly exploit it. In other words, a pure NSA trapdoor would have the property that inserting it gives the NSA access but does not weaken the security of users against attack by any other potential adversary.

The equities of a pure NSA trapdoor might be an interesting topic for debate, but that debate is not directly relevant here because all of the suspected NSA trapdoors in NIST standards are impure trapdoors. In every case discussed below, if the suspected trapdoor does exist, its existence reduces the security of users against attack by a other adversaries, including organized crime groups or foreign intelligence services. Making the standards trapdoor-proof would make users more secure against these adversaries.

Assessment of Specific NIST Standards and Guidelines

NIST provided the CoV with information regarding 23 NIST cryptographic documents: five Federal Information Processing Standards (FIPS), and eighteen Series 800 NIST Special Publications (SP). These are listed in Appendix A.

After reviewing the historical background on these documents, the CoV focused its attention on three issues:

1. in SP 800-90A (Recommendation for Random Number Generation Using Deterministic Random Bit Generators), the inclusion of the DUAL_EC pseudorandom bit generator algorithm, and the choice of recommended values for the public parameters P and Q in DUAL_EC;
2. in FIPS 186 (Digital Signature Standard), the choice of elliptic curves recommended in ECDSA (Elliptic Curve Digital Signature Algorithm)[7]; and
3. in the SP 800-38 series (Recommendation for Block Cipher Modes of Operation), decisions to recommend specific cipher modes for specific uses despite evidence of security weaknesses.

[7] The same curves are used for key agreement in SP 800-56A, so the discussion of FIPS 186 curves in this report applies generally to SP 800-56A as well.

DUAL_EC in SP 800-90A: What Went Wrong

NIST Special Publication 800-90A specified standards for generating pseudorandom bits. SP 800-90A is based on an earlier private sector standard known as X9.82 Part 3. The following timeline summarizes the two interlocking processes:

1998: X9 group begins work on X9.82 Part 3
2003: DUAL_EC added to X9.82 Part 3
2003: NIST begins its participation in X9.82
2005: NIST begins its SP 800-90 process
2006: NIST publishes SP 800-90
2007: X9 approves final version of X9.82 Part 3
2008: NIST publishes SP 800-90A
2013: NIST recommends against use of DUAL_EC, reopens SP 800-90A[8]

SP 800-90A specifies methods for constructing a pseudorandom generator, which is a critical component in cryptography, because it is the source from which secret cryptographic keys are derived. If an adversary can predict the output of a system's pseudorandom generator, it can defeat most or all of the encryption used by the system.

SP 800-90A gave a choice of four core bit generation algorithms, including one called DUAL_EC that is based on elliptic-curve mathematics. Based on information available now, it appears highly likely that DUAL_EC contained a trapdoor created by NSA, allowing NSA to predict the output of a DUAL_EC-based generator. The evidence I have seen indicates that NIST believed at the time, in good faith, that there was not a trapdoor. However, NIST could and should have prevented even the possibility of a trapdoor.

In discussion with the CoV, NIST personnel were very forthcoming about the history and the factors that led to decisions about DUAL_EC. NIST's in-person presentation to the CoV about DUAL_EC was comprehensive, thoughtful, and frank.

The bottom line is that NIST failed to exercise independent judgment but instead deferred extensively to NSA with regard to DUAL_EC. After DUAL_EC was proposed, two major red flags emerged. Either one should have caused NIST to remove DUAL_EC from the standard, but in both cases NIST deferred to NSA requests to keep DUAL_EC.

Red Flag #1: Biased Output. In 2006, researchers showed that the output of DUAL_EC was biased so that DUAL_EC failed to pass statistical tests for randomness. This failure to meet a basic requirement for pseudorandom generators should have disqualified DUAL_EC. At the urging of NSA, NIST agreed to include DUAL_EC in the standard despite the bias issue. Although the bias problem could have been fixed (by discarding some of the bits produced by the generator), NSA asserted that the fix was not needed, and NIST accepted this assertion.

[8] NIST took these actions a few days after the public disclosure of NSA's "SIGINT Enabling" program, which caused many commentators to conclude that NSA probably had a trapdoor to DUAL_EC. See http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf

It was discovered later that had NIST addressed the bias problem by changing the standard to discard some of the biased bits, this would have had the side effect of eliminating the potential trapdoor in DUAL_EC. This might be a reason why NSA argued against addressing the bias problem.

Red Flag #2: Potential trapdoor. In 2005, researchers discovered a potential trapdoor in DUAL_EC. The DUAL_EC algorithm uses two public parameters, P and Q. It is believed that DUAL_EC is secure if P and Q are chosen randomly. But if a party is allowed to choose P and Q, that party can choose P and Q in such a way that the party is able to predict the generator's output. This trapdoor vulnerability was discussed several times during the standardization process. NIST, as part of the X9.82 Part 3 group, learned of the trapdoor vulnerability in 2005 but did not address it adequately.

In light of this known trapdoor possibility, NIST should not have allowed NSA to provide the values of P and Q that were recommended in the standard. NIST knew at the time that its actions would allow NSA to have a trapdoor into the standard. NIST trusted NSA not to create a trapdoor, which was a serious mistake.

At a minimum, NIST should have asked NSA to provide evidence that these parameters were generated in a verifiably random way. In fact, the appendix to SP 800-90A that allows implementers to specify alternative parameters requires precisely such a check at initialization time. It was an error for NIST not to require a similar check for the default P and Q values recommended in the standard.

A NIST person aptly summarized this error to the CoV by saying that NIST had asked the wrong question. It had asked, "Do we think there is a trapdoor?" when it should have asked, "Should we include an algorithm in our standards that could have a trapdoor?"[9]

Even if NIST's trust in NSA not to trapdoor the standard had been entirely justified---even if NIST knew somehow that there was absolutely no chance that NSA had created a trapdoor---this decision would still have been a mistake, because even the appearance of a possible NSA trapdoor undermined the goal of widespread adoption of the standard. Indeed, many cryptographers concluded, based on publicly available information at the time, that DUAL_EC was suspect and should not be used.

[9] NIST's initial approach to the possibility of a trapdoor is illustrated by an exchange in 2007. Bruce Schneier wrote a column in Wired pointing to the possibility of an NSA trapdoor in DUAL_EC (https://www.schneier.com/essay-198.html). NIST replied with a letter saying that "We have no evidence that someone knows the existence of the 'secret numbers' that Dan Shumow and Niels Ferguson have shown would provide advance information about the pseudorandom numbers that Dual_EC_DRBG would generate. Therefore, we have no plans to withdraw the algorithm at this time." (https://github.com/matthewdgreen/nistfoia/blob/master/107%20-%20Dr.%20Schneier%20Letter%20-%20Wired%20Commentary.pdf?raw=true)

A better approach, if DUAL_EC was going to be kept in the standard at all, would have been for NIST to conduct a public "ceremony" to choose new pseudorandom values for P and Q, using the "verifiably random point generation" procedure specified in Appendix A.2.1 of SP 800-90A. By demonstrating that P and Q were indeed chosen at random, NIST could have dispelled the possibility, and the appearance of a possibility, of a trapdoor. NIST could easily have done this.

Alternatively, NIST could have made the standard agnostic as to the choice of parameters, recommending only that the parameters be chosen pseudorandomly as described in Appendix A.2.1. Although the standard did allow the use of alternative parameters generated in this way, it made the NSA-chosen parameters the default, and it did not explain why it might be desirable to use different parameters.

Recommendation: *NIST should not try to fix the DUAL_EC algorithm in SP 800-90A but should instead reissue the standard with DUAL_EC removed.*

If DUAL_EC was going to be included in the standard, the best approach to doing so would have been to modify DUAL_EC to eliminate the possibility of a trapdoor. For example, this could have been done by adding a step at the end of DUAL_EC pipeline that passed the bits produced by the generator through a one-way transformation, which would have prevented a trapdoor attacker from inferring internal states of the generator, thereby thwarting the trapdoor attack.

Doing this would have had the additional benefit of protecting users against the possibility of a software vendor creating a trapdoor by choosing its own P and Q. The DUAL_EC standard as presently written allows vendors to substitute their own P and Q values, which gives the vendor (or a malicious insider at the vendor) a trapdoor opportunity. A trapdoor-proof standard would prevent this.

Recommendation: *NIST should aim to create standards that resist trapdoors at the technical level. To the extent that a standard cannot avoid the possibility of a trapdoor controlled by any party, including NIST itself, the standard should disclose this possibility and give clear guidance on how to mitigate the resulting risk.*

Several factors contributed to NIST's errors on DUAL_EC. One contributing factor was the dual-track process, in which X9 first created a standard and then NIST based its own standard on X9's product. X9 used a collaborative process in which NIST and NSA participated as two members of a larger committee, an arrangement that made sense for X9's purpose. Successful standards committees operate in a spirit of compromise, and they will often accept into the standard a proposal that is backed by just one strong-willed member but "seems harmless." NIST standards are supposed to be made in a different way, with the community providing extensive input but NIST exercising its own judgment. In adapting the X9 standard into a NIST standard, NIST took for granted too much of the X9 standard's content.[10]

[10] The tension between the X9 process and NIST's mandate to exercise independent judgment in its own standards was exacerbated by the fact that the X9 process started several years before the NIST process. During the drafting of the X9 standard, some companies began implementing the X9 version, and these

Another contributing factor was limited staffing at NIST. NIST employees were pressed for time and had to divide effort among many projects, reducing the amount and consistency of effort they could devote to DUAL_EC. In addition, at the time NIST had nobody on staff with expertise in elliptic curves.[11] NSA's vastly superior expertise on elliptic curves led NIST to defer to NSA regarding DUAL_EC, while NIST people spent more of their limited time on other parts of the standard that were closer to their expertise.

Recommendation: *NIST should continue to increase the depth and breadth of its cryptographic expertise, in order to maximize NIST's capacity to exercise independent technical judgment on cryptographic security standards. NIST should take three steps toward this goal:*

- *NIST should do what it can within current budgetary constraints to increase its expert cryptographic standards staff;*
- *NIST should work within the Federal budget process to seek increased funding for its cryptographic standards work; and*
- *NIST should build relationships with independent cryptography experts, especially in technical areas where NIST's expertise is thinner.*

Elliptic Curves in FIPS 186: Unanswered Questions

NIST's digital signature standard, FIPS 186, includes a specification of the Elliptic Curve Digital Signature Algorithm (ECDSA)[12]. ECDSA relies on elliptic curves, which are mathematical constructs with certain efficiency advantages for cryptography. FIPS 186 recommends fifteen specific elliptic curves for use with ECDSA. The same curves are recommended for use in key exchange, in SP 800-56A. These curves were chosen by NSA, as described below. There is concern in some circles that NSA might have chosen curves that allow it to trapdoor the standard.

It will be useful to lay a bit of groundwork before discussing how curves were chosen. There is a large universe of elliptic curves, but many of them are "weak" or unsuitable for cryptographic use. A curve can be tested to see if it is known to be weak. We can call a curve "believed-strong" if it passes these tests.

FIPS 186 describes a pseudorandom procedure for choosing curves. The procedure starts with a seed, which is supposed to be chosen randomly, and uses a deterministic algorithm based on the seed to compute parameters that describe a curve. If the resulting curve is weak, it is discarded and the process is repeated until a believed-strong curve is generated.

---

existing implementations became the basis for later arguments against NIST deviating from the X9 version.

[11] I understand that NIST now has an elliptic curve expert on staff.

[12] ECDSA was added in FIPS 186-2, in 2000.

This procedure was used to generate the recommended curves in FIPS 186, but NIST allowed NSA to choose the seeds. This meant that NSA had some control over which curves were chosen. Because of the properties of the algorithm that maps a seed to a curve, NSA was not able to choose precisely which curve was used.

However, suppose that NSA had secret knowledge that a particular subset of the believed-strong curves were actually weak, and that this knowledge would allow NSA to have a trapdoor should one of the curves in this secretly weak subset be chosen. Then NSA could secretly generate many seeds, see which curves resulted from each of these seeds, and then supply NIST with a seed that generates a secretly weak curve. If one in a million of the believed-strong curves were secretly weak, then NSA would have to try a million seeds, on average, to find a weak curve and thereby create a trapdoor.

There is no evidence that NSA had secret knowledge of weak curves, but this possibility cannot be ruled out either, given the very considerable elliptic curve expertise at NSA. In any case, NIST could easily have eliminated the possibility of an NSA trapdoor by generating the seeds itself, in a way designed to foster public confidence.

If NSA did create a trapdoor of this type, this would have made the standard less secure for all users. The secret knowledge that enabled the NSA trapdoor would be in the nature of mathematical knowledge that had been discovered by NSA researchers. If a researcher working for some adversarial party discovered the same mathematical result, that party would be able to use the trapdoor as well. The creation of the trapdoor would have put all users at risk of being exploited due to such a discovery.

NIST can eliminate any doubt by generating a fresh set of curves now, choosing seeds by a demonstrably random public process, then using those seeds to generate new curves. This has the additional advantage that the set of believed-good curves can be adjusted to account for advances in cryptographic knowledge regarding elliptic curves that have occurred since the original curves were generated.[13]

NIST can recommend the use of the new curves over the old ones, but it probably makes sense to allow use of the old curves for reasons of backward compatibility.

Recommendation: *NIST should generate a new set of elliptic curves for use with ECDSA in FIPS 186. These should be generated by a public process such that the cryptographic community can be confident that the resulting curves were chosen pseudorandomly from among a set of high-quality curves. The set of high-quality curves should be described precisely in the standard, and should incorporate the latest knowledge about elliptic curves.*

Another problem with FIPS 186 and some other NIST standards is that they incorporate by reference some material from privately-published standards that are not freely available to the

[13] For example, it has been discovered that curves recommended in FIPS 186 are subject to a certain type of side-channel attack in some scenarios. New curves can be chosen that do not suffer from such attacks.

public. This practice is questionable because NIST is mandating a standard that requires payment to a private party. More importantly, this practice reduces the security of NIST standards by creating a barrier to outside experts who might want to study the standard. One of the strengths of NIST's process is the way it encourages participation by the cryptographic community to find weaknesses and suggest improvements. Incorporating non-public material into a standard undermines this process and harms security.

Recommendation: *NIST should not include non-public material in its standards. If it is necessary to include such material, NIST should make necessary arrangements so that the standard is available to everyone who wants to participate in studying or implementing the standard, throughout the standard's lifetime.*

SP 800-38 Cipher Modes: Coping with Tradeoffs

NIST's SP 800-38 series of recommendations describes cipher modes, which are methods for using an existing block cipher (such as the Advanced Encryption Standard) to solve particular cryptographic problems. In choosing which cipher modes to recommend, NIST had to make some difficult decisions, sometimes trading off security against other goals such as backward compatibility and consistency with existing private-sector standards. NIST has stated its rationales for these choices.

In NIST's cipher mode work, the risk of an NSA-related problem is highest in cases where NSA played a role in designing a cipher mode, and that mode lacks a detailed, public security analysis. Both of these conditions apply to the KW (AES Key Wrap) and KWP (AES Key Wrap with Padding) modes specified in SP 800-38F.

Recommendation: *NIST should evaluate whether there is sufficient reason to reopen the decision to recommend the KW and KWP cipher modes in SP 800-38F.*

Path Forward

NIST's credibility with the cryptographic community cannot be rebuilt overnight. But rebuilding that credibility is critical to advancing NIST's mission and benefiting technology users in the U.S. and overseas.

NIST has several important factors in its favor. NIST's cryptographic staff are skilled and remain dedicated to its mission. Although the cryptographic community believes---probably correctly---that at least one NIST standard contained a trapdoor, the community also believes that NIST did not want such a trapdoor and did not knowingly allow it. The community believes that NIST is trying to produce secure standards; and the community is willing to be convinced over time that NIST has taken the necessary steps to protect more effectively against subversion of its standards and processes.

The recommendations in this report aim to help NIST regain the community's trust. I believe these recommendations are generally consistent with what NIST is already planning to do. NIST has clearly learned from its recent experience and is moving in the right direction. The integrity of cryptographic standards must remain a high priority for NIST.

List of Recommendations to NIST

Recommendation: *NIST should reiterate clearly the importance of fostering widespread justified confidence in NIST's cryptographic standards and recommendations. Widespread confidence advances NIST's goals, enabling better security for all users of NIST standards.*

Recommendation*: Because of NSA's SIGINT mission, NIST should be very careful in its interactions with NSA regarding standards. NIST should draw on NSA's expertise, but NIST must not defer to NSA on security-relevant decisions. NIST itself, and the cryptographic community that looks to NIST's standards, must be able to conclude with confidence that NSA did not have any opportunity to undermine any NIST standard.*

Recommendation*: NIST should review its Memorandum of Understanding with NSA to make sure that the MOU is consistent with the standard-making autonomy granted to NIST by statute.*

Recommendation*: NIST should not try to fix the DUAL_EC algorithm in SP 800-90A but should instead reissue the standard with DUAL_EC removed.*

Recommendation*: NIST should aim to create standards that resist trapdoors at the technical level. To the extent that a standard cannot avoid the possibility of a trapdoor controlled by any party, including NIST itself, the standard should disclose this possibility and give clear guidance on how to mitigate the resulting risk.*

Recommendation*: NIST should continue to increase the depth and breadth of its cryptographic expertise, in order to maximize NIST's capacity to exercise independent technical judgment on cryptographic security standards. NIST should take three steps toward this goal:*

- *NIST should do what it can within current budgetary constraints to increase its expert cryptographic standards staff;*
- *NIST should work within the Federal budget process to seek increased funding for its cryptographic standards work; and*
- *NIST should build relationships with independent cryptography experts, especially in technical areas where NIST's expertise is thinner.*

Recommendation*: NIST should generate a new set of elliptic curves for use with ECDSA in FIPS 186. These should be generated by a public process such that the cryptographic community can be confident that the resulting curves were chosen pseudorandomly from among a set of high-quality curves. The set of high-quality curves should be described precisely in the standard, and should incorporate the latest knowledge about elliptic curves.*

Recommendation: *NIST should not include non-public material in its standards. If it is necessary to include such material, NIST should make necessary arrangements so that the standard is available to everyone who wants to participate in studying or implementing the standard, throughout the standard's lifetime.*

Recommendation: *NIST should evaluate whether there is sufficient reason to reopen the decision to recommend the KW and KWP cipher modes in SP 800-38F.*

Appendix A: Relevant NIST Standards and Special Publications

Federal Information Processing Standards (FIPS)

- FIPS 180: Secure Hash Standard (SHS)
- FIPS 185: Escrowed Encryption Standard (EES)
- FIPS 186: Digital Signature Standard
- FIPS 197: Advanced Encryption Standard
- FIPS 198: The Keyed-Hash Message Authentication Code (HMAC)

800 Series NIST Special Publications (SP)

- SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques
- SP 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
- SP 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
- SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
- SP 800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices
- SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
- SP 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
- SP 800-56B: Recommendation for Pair-Wise Key Establishment Schemes: Using Integer Factorization Cryptography
- SP 800-56C: Recommendation for Key Derivation through Extraction-then-Expansion
- SP 800-57: Recommendation for Key Management
- SP 800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher
- SP 800-90A: Recommendation for Random Number Generation Using Deterministic Random Bit Generators
- SP 800-106: Randomized Hashing for Digital Signatures
- SP 800-108: Recommendation for Key Derivation Using Pseudorandom Functions
- SP 800-131A: Transitions: Recommendation for Transitioning the Use of
- Cryptographic Algorithms and Key Lengths
- SP 800-132: Recommendation for Password-Based Key Derivation Part 1: Storage Applications
- SP 800-133: Recommendation for Cryptographic Key Generation

- SP 800-135: Recommendation for Existing Application-Specific Key Derivation Functions

Report of Steven B. Lipner*

to the

NIST VCAT Subcommittee on Cybersecurity

6 June 2014

Introduction

The Committee of Visitors (CoV) was charged to review NIST's current cryptographic standards and guidelines development process and provide feedback on the principles that should drive standards and guidelines development, the processes for effectively engaging the cryptographic community and communicating with stakeholders, and NIST's ability to fulfill its commitment to technical excellence. The committee was also charged to assess NIST cryptographic materials, noting when they adhere to or diverge from those principles and processes.

In conducting my review and assessment, I relied heavily on the documents and presentations that NIST prepared and presented to the CoV as well as other documents that are available from the NIST website. I also relied on my previous experience with and observations of past controversies related to NIST's development of cryptographic standards. These observations go back to the creation and standardization of the Data Encryption Standard in the late 1970s, and encompass the "crypto wars" over export controls and escrowed encryption that occurred in the late 1980s and early 1990s.

This review is provided from the perspective of more than forty years of work in cybersecurity, but not from the perspective of a cryptographer. Thus I have focused on principles, process, and the public and market concerns that I've observed, but not on specific issues related to encryption technology. If such issues need to be raised, I trust that other committee members who are cryptographers will raise them.

Background and Motivation

The Snowden Allegations and Dual EC DRBG

The issue that led to the formation of the CoV was worldwide concern about the claim in the Snowden disclosures that NSA had caused NIST to weaken encryption standards that were issued by NIST and adopted by Information Technology (IT) vendors and users. The presumption underlying the concern was that while wide adoption of such weakened standards would allow NSA more easily to decrypt intercepted communications of terrorists or hostile governments it targeted, the privacy and integrity of *any* individual's or organization's information could also be jeopardized by products that implemented such weakened standards..

Further, weakened encryption might be discovered and exploited by organizations other than NSA. Thus if encryption standards were weakened, innocent individuals and organizations who use encryption to protect their commercial information from theft or to protect themselves from repressive governments or simply to ensure their privacy might find that their information at risk.

* Steven B. Lipner is partner director of program management at Microsoft Corporation. The views expressed in this report do not necessarily represent the views of Microsoft Corporation.

More broadly, given the pervasiveness of US-developed IT products that implement NIST security standards, an action by NIST or NSA to weaken encryption standards in the name of US national security could undermine trust in the Internet generally. The reaction to the Snowden allegations illustrates this point: foreign governments and enterprises that use commercial IT products that implement NIST standards were particularly concerned that their communications and data might be subject to disclosure.

The Snowden allegations have not (to my knowledge) been confirmed but the encryption community began almost immediately to speculate that the Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC DRBG) that is described as part of NIST SP 800-90 was the standard in question. A weakness in this algorithm would be very serious for IT users, since an expected use of the algorithm would be generation of cryptographic keys and weak (easily determined) keys undermine the effectiveness of even strong encryption algorithms.

In response to concerns about Dual EC DRBG, NIST withdrew the algorithm from SP 800-90.

Ancient History

While the concerns about Dual EC DRBG and the Snowden allegations are very current, they are by no means the first example of public concerns about NSA's influence on the development of NIST encryption standards. The first concern coincided with NIST's first effort at developing an encryption standard. In the mid-1970s, NIST consulted with NSA as it was developing the Data Encryption Standard (FIPS 46 or DES) based on IBM's Lucifer encryption algorithm. The version of DES that NIST standardized incorporated a much shorter key length than IBM's Lucifer algorithm on which it was based (56 bits rather than 128) and a set of unexplained internal changes to a structure referred to as the S-boxes.

Speculation about DES centered on the shorter key – an apparent reduction in the strength of the algorithm – and on the possibility that the new S-boxes weakened DES to have an effective strength of even less than 56 bits. Eventually, the cryptographic community came to the conclusion that the changes to the S-boxes protected DES from a technique called differential cryptanalysis that was only discovered by the cryptographic research community well after DES was standardized. To an adversary who knew about differential cryptanalysis, the strength of Lucifer with the original S-boxes was significantly less than 56 bits. The reduction in key length of DES from Lucifer's 128 bits to 56 bits in fact reduced the strength of the algorithm, but also facilitated hardware implementations of DES in an era when semiconductor technology was much less advanced than it is today.

In the late 1980s, use of the Internet was increasing and with it, user concerns about network security and the need for encryption. Public key encryption had been developed by the cryptographic research community, and been determined to be effective both for digitally signing information to protect its integrity and for securely distributing DES keys that would be used to protect confidentiality. IT users encouraged NIST to standardize a public key encryption algorithm for commercial and unclassified government use.

The public key encryption algorithm that NIST eventually standardized as FIPS 186, the Digital Signature Standard (DSS), was developed by NSA and usable for digital signature (authentication) but not to distribute DES keys or to protect the secrecy of information. Speculation in the cryptographic research community and among vendors (I was one of the latter) was that the DSS was designed as it was to slow the adoption of encryption for secrecy. The private sector almost universally chose to adopt the RSA

algorithm (which could be used for key distribution for confidentiality as well as digital signature) rather than DSS, and actual use of DSS remained minimal.

In the early 1990s, AT&T designed and prepared to sell a portable device that used DES to encrypt users' voice telephone calls. Before AT&T released the DES device widely, their plans changed and they began producing of a version of the device that implemented "escrowed encryption" with split master keys held by two agencies of the US government. This device featured a (then) classified encryption algorithm with an 80-bit key length (stronger than DES) that was implemented by a sealed and secret encryption chip. If a court ordered a wiretap against the user of a specific Clipper-enabled device, the holders of the master keys would cooperate (if legally required) to release to law enforcement a key that would allow communications by that device to be decrypted. NSA and FBI conducted outreach and advocacy for escrowed encryption as a way of protecting users' information with strong encryption while preserving the option for law enforcement to gain access to the information when necessary and under court order. One of the attractions of escrowed encryption was that escrowed devices, unlike those that incorporated DES, could be exported from the United States with few restrictions.

NIST became involved in the escrowed encryption initiative as one of the government agencies that held parts of the split master key. NIST also standardized escrowed encryption components as FIPS 185, the Escrowed Encryption Standard although the technical details of escrowed encryption as implemented in the AT&T device were classified and omitted from the standard. The private sector and some in Congress strongly opposed the use of escrowed encryption, and by early this century, both escrowed encryption and effective export controls over commercial encryption (i.e. encryption controlled under the Export Administration Regulations rather than under the International Trafficking in Arms Regulations) were things of the past.

NIST, NSA, and Reputation

The common thread among the incidents discussed above is suspicion that NSA may have interfered with NIST-developed encryption standards with the aim of weakening them and facilitating NSA's intelligence mission. The suspicion has survived for almost forty years, fueled by periodic initiatives such as EES and most recently by the Snowden disclosures.

Suspicions of NSA intervention in NIST standards in support of the NSA intelligence mission have a negative effect on NIST's reputation and the credibility of the standards NIST develops. Those suspicions not only cause cryptographers and researchers to question NIST's credibility, but in a world where Internet security is critical to IT users – businesses, consumers, and governments – they also have a negative effect on the credibility of US industry that implements those standards and thus on international competitiveness. Thus there are multiple reasons for NIST to protect the reputation and integrity of its standards, and to avoid any taint of suspicion that NIST standards are developed in such a way as to facilitate US intelligence gathering.

Observations on NIST Practices

NIST's discussion of the history of the Dual EC DRBG was especially revealing. While there were no clear signs of a deliberate attempt by NIST – or NSA – to undermine the security of the algorithm, NIST's discussion revealed and acknowledged numerous process shortcomings that allowed a potentially weak algorithm to be standardized. Some of these shortcomings include:

- Because ANSI standards are only available by subscription or payment, NIST's decision to collaborate with ANSI X9 on the development of the DRBG guidelines and to participate in standard development in X9 made it difficult to seek broad (public) review of the initial versions of the emerging standard. Because the initial standard was not a NIST standard, this might not have been a major issue unto itself.
- When NIST decided to release a DRBG standard as a NIST guideline (SP 800-90) elements of the ANSI DRBG standard appear to have been brought over to the NIST draft without complete review or vetting.
- NSA advised NIST that the constants associated with the Dual EC DRBG were generated in a secure, classified way. While this statement may be literally true, in retrospect it made the process of developing the standard much less transparent, and thus a potential subject for concern. Given that there were alternative ways of generating the constants that were secure and could be made public, there was no clear justification for this element of secrecy.
- NSA sought to include the Dual EC DRBG in SP 800-90 so that existing devices that implemented the algorithm would be eligible for FIPS validation. This may have been a sufficient reason for including the algorithm or it may not – but there was no sign that NIST exercised its authority and autonomy to question the importance of including the algorithm given the uncertainties about generation of the constants.

Cryptographers raised questions about the origin and security of the constants in the Dual EC DRBG and about the properties of the random numbers it generated. These questions led to discussions in cryptographic conferences and in ANSI X9, but in the end, the Dual EC DRBG algorithm remained part of SP 800-90. The NIST responses to the questions were informal and incompletely tracked and documented, with the result that there is not a clear record that inputs were considered, issues resolved, and decisions made. The process was informal and ad hoc, and when questions were raised about Dual EC DRBG in the aftermath of the Snowden allegations, it was difficult for NIST to document what decisions were made and why they were made.

NIST also discussed the development of FIPS 186, the Digital Signature Standard, focusing on the choice of elliptic curves, and SP 800-38, Block Cipher Modes of Operation. For both elliptic curves and some of the block cipher modes, there are options that allow proof of the security of the curve or mode under a set of clear assumptions. The NIST elliptic curves in fact support such proof while some of the block cipher modes do not. A decision by NIST to prefer algorithms where proof is feasible would have helped to forestall subsequent questions about the choices NIST made.

Given the compressed schedule of the briefings to the CoV and the absence of controversy associated with the subject, NIST did not discuss the cryptographic competitions that led to the standardization of the Advanced Encryption Standard (AES – FIPS 197) and the ongoing standardization of the new Secure Hash Algorithm (SHA-3). However NIST did summarize the competitions in its briefing papers to the CoV and I followed the progress of both competitions in my role as an industry security engineering manager. Both competitions attracted worldwide participation and attention from the academic community and industry and were widely seen as fair and well-executed. These competitions organized and managed by NIST are examples of best practices in the development of cryptographic standards.

During their briefings to the CoV, NIST staff referred to periods when they lacked expertise in some forms of cryptography and cryptanalysis, and also to growing expertise and the addition of new expert

staff. The growth of the size and competence of NIST's Cryptographic Technology Group over the last forty years is an important trend and one whose continuation will be important to NIST's ability to meet its responsibilities under law.

Recommended Principles

NIST has identified a set of principles that guide its work on cryptographic standards in the draft NISTIR 7977, NIST Cryptographic Standards and Guidelines Development Process. Those standards are sound but they are stated in general terms and do not focus specifically on the issues of integrity of process that have arisen in the aftermath of the Snowden allegations. Given the seriousness of those allegations and the threat to NIST's reputation, I believe that there's a need for a very clear set of principles that directly address the integrity of NIST's cryptographic standards and guidelines. I have proposed such a set of principles below:

- Security first: When NIST issues a standard or guideline whose primary purpose is security, the security of that standard or guideline (e.g. the security of the algorithm, protocol, process, or design that is standardized) should be treated as the top priority. The standard or guideline should be clear about what protections are offered or threats mitigated, and it should be effective at providing those protections or mitigating those threats "as advertised." This principle also requires that design of security standards and guidelines be conservative with minimal assumptions or issues left to faith or chance.
- Transparency of process: Both before and after a security standard or guideline is adopted, NIST should be open about what steps were followed, what authorities were consulted or reviews sought, what comments were received, and what actions or resolutions reached. There should be no loose ends or untraceable actions in the standard review process.
- Transparency of product: NIST security standards and guidelines should not incorporate concealed or secret features or attributes. This principle would have precluded NIST's standardization of the Skipjack algorithm in the EES, for example, and it would also forbid the weakness that was claimed to affect the Dual EC DRBG.
- Authority and autonomy: The Computer Security Act of 1987 and the Federal Information Security Management Act give NIST authority and responsibility for setting security standards for unclassified systems subject to the approval of those standards by the Secretary of Commerce and to their potential disapproval or modification by the President. While NIST is required to coordinate with other agencies including NSA, NIST has the authority to set standards for unclassified systems and should exercise that authority. This principle also implies that NIST should have the competence and resources to exercise it authority.
- Global acceptability: Providers of IT products and services implement NIST security standards and guidelines and then sell or license products or services worldwide. International concerns about the soundness or integrity of NIST security standards can have a significant negative effect on the competitiveness of US industry. Thus NIST should ensure that its security standards will be seen as trustworthy by IT users worldwide.
- Fair treatment of equities: NIST's efforts must be focused exclusively on the development of secure standards and algorithms for use by the unclassified elements of the US government. NSA seeks to balance between a security mission that supports both the national security and (under the Computer Security Act of 1987 and FISMA) unclassified elements of the US

government and an intelligence mission. As the example of DES appears to make clear, NSA's input can be extremely valuable to the soundness of a standard or guideline. But in consulting with NSA and considering NSA's input, NIST should strive to adhere to the other principles listed above. When conflicts arise between NIST and NSA, NIST should not hesitate to escalate them within the executive branch to levels of government that can fairly take a long-term perspective and consider the tradeoffs among considerations such as national security, economic competitiveness, and national reputation.

Recommendations

In this section, I will enumerate my recommendations and identify in parentheses the principles that they support. If the rationale for a recommendation is not evident, I will articulate it below.

- NIST should only allow its responsibility for setting cryptographic standards to be used to improve the security of IT users, and it should do so in ways that meet users' needs. (Security first) This would imply that NIST should not attempt to satisfy users with a digital signature solution when user demand is clearly for a key distribution algorithm.
- NIST should not hesitate to seek NSA's advice as it is evaluating decisions about cryptographic standards and guidelines. (Security first) While NIST should not be bound to accept such advice, NSA brings vast expertise in cryptography and it would be shortsighted for NIST not to avail itself of that expertise. Of course, NIST should have sufficient in-house expertise to understand and assess the advice offered, and to know when to accept and when to reject it. (Authority and autonomy)
- NIST should ensure that feedback and concerns about evolving cryptographic standards are tracked and documented, and that all are resolved before a standard is issued. (Transparency of process) This recommendation does not mean that NIST must become overly bureaucratic, but it does suggest a significant improvement in record-keeping and workflow management. The diligent use of a workflow management or bug-tracking system such as is used by large software projects would probably help NIST ensure that no concerns drop through a crack and no essential feedback goes unresolved. NIST management should review the status of feedback and concerns before key milestones in the standardization process to help ensure against errors, oversights, and attempts to manipulate the standard-setting process.
- NIST should use open cryptographic competitions to select cryptographic standards where feasible. (Transparency of process, Transparency of product, Global acceptability) Such competitions are widely respected and a best practice, and the reaction to standards that were selected by past competitions has been universally positive.
- NIST should ensure that cryptographic evaluations of new cryptographic standards are conducted and released to the public. (Security first, Transparency of process, Global acceptability) These evaluations will communicate the technical reasons why NIST believes the standards to be secure, and will also help to ensure that NIST itself clearly understands the rationale behind the standard. If a standard is also the subject of a classified evaluation by NSA, NIST may consider that evaluation in the process of developing the standard, but should still ensure that an unclassified evaluation whose results are consistent with those of the classified evaluation is released.

- NIST should ensure that there are no secret or undocumented components or constants in its cryptographic standards whose origin and effectiveness cannot be explained. (Transparency of product) This recommendation would preclude the issuance of the EES with its reliance on the then-secret Skipjack algorithm as well as the Dual EC DRBG with its reliance on an elliptic curves whose origin was undocumented and whose security could not be verified.
- NIST personnel who are assigned to the development of cryptographic standards should always operate from a position of authority. (Authority and autonomy) They should not allow their personal relationships or relative levels of rank or experience to cause them to defer to individuals from other agencies (especially NSA). NIST personnel should make decisions based on technical arguments and considerations of strong security, and NIST leadership should be prepared to engage on challenges to the principle of Authority and autonomy when decisions of NIST personnel are challenged, and to apply the principle of Fair treatment of equities when appropriate.
- Closely related to the recommendation above, NIST should ensure that the Cryptographic Technology Group is resourced sufficiently to develop the standards and guidelines that the United States and its industry require, and to be expert in the cryptographic technologies that will be required to protect unclassified information. (Authority and autonomy) NIST may wish to consider supplementing its full-time staff with visiting experts from industry or academia who serve as part-time or temporary staff to participate in NIST programs and share their knowledge and expertise with NIST staff, or with staff from the new cybersecurity FFRDC, but this measure should be viewed as a supplement to a strong staff of in-house experts, not a substitute.
- NIST may wish to consider establishing an international advisory panel of cryptography researchers to provide input to its standards development activities and to the operation of the Cryptographic Technology Group. (Global acceptability, Authority and autonomy) Such a panel could advise NIST on emerging trends in cryptography and cryptanalysis and help guide the evolution of the Cryptographic Technology Group. It could also help to channel talented recruits to NIST and, if international in membership, could help build worldwide confidence in NIST's cryptographic standards and guidelines, and thus in US IT products that implement them. I phrase this recommendation as "may" rather than "should" because world-class cryptographers may wish to participate in NIST cryptographic competitions rather than serve on an advisory panel, and fairness suggests that panel members be excluded from competitions.
- NIST senior leadership should work with the Executive Office of the President to ensure that conflicts over development of cryptographic standards are subject to escalation under appropriate White House-led interagency processes. (Fair treatment of equities) NIST should not hesitate to avail itself of these processes in the event that they are pressed by NSA (or any other agency) to make a decision about cryptographic standards or guidelines that would violate one of the principles listed above.
- NIST senior leadership should foster a culture inside NIST that supports and adheres to these principles. If personnel do not see NIST leadership following these principles and, when necessary, challenging inappropriate influences on cryptographic standards, neither the principles nor NIST's legislated cybersecurity mission will succeed.

Adoption of the recommendations above will help to reinforce the credibility and quality of NIST's cryptographic standards and guidelines. It will also help to improve the security of the nation's unclassified IT systems and the international competitiveness of US industry.

Comments on the NIST Cryptographic Standards and Guidelines Development Program

VERSION 1.0

Bart Preneel
KU Leuven COSIC and iMinds
Dept. Electrical Engineering-ESAT
Kasteelpark Arenberg 10, bus 2452, B-3001 Leuven, Belgium
firstname.lastname@esat.kuleuven.be

July 5, 2014

Contents

[1]This document was originally published as SP 800-90; subsequently it was planned to add parts 90B and 90C and this version was renamed 90A; parts B and C are still under development.

1 Introduction

As member of the Committee of Visitors (COV), I was asked to

- 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's ability to fulfill its commitment to technical excellence.

- Assess NIST cryptographic materials, noting when they adhere to or diverge from those principles and processes.

This document is my individual report to the VCAT Subcommittee on Cybersecurity for their consideration in the development of a final report to the VCAT and any subsequent recommendations to NIST.

The following documents have been taken into account in the preparation of this report:

- Charge to the Committee of Visitors (COV) NIST Cryptographic Standards and Guidelines Development Program Briefing Book, 13 May 2014.

- Computer Security Act, 1987

- Administrative Procedure Act, par. 553, Rule Making.

- Memorandum of Understanding between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100-235, 1989.

- Memorandum of Understanding 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, 2010.

- Circular No. A-119, Re Memorandum for Heads of Executive Departments and Agencies, February 10, 1998, `http://www.nist.gov/standardsgov/omba119.cfm`

- NIST Cryptographic Standards and Guidelines Development Process (Draft), NISTIR 7977, February 2014 and public comments received on this draft.
- Background-Public Concerns and Initial Steps (slide set)
- Dual EC in X9.82 and SP 800-90 (slide set)
- Development of SP 800-38 Series for Block Cipher Modes (slide set)
- Correspondence between Alan Grayson (Member of Congress) and Patrick D. Gallagher (Under Secretary of Commerce for Standards and Technology)

Because of the tight schedule, it has not been possible to review all cryptographic standards and guidelines published by NIST. Moreover, it has also not been possible to review the internal processes. In particular, I have not reviewed any internal documents from NIST or ANSI X9F1 related to the development of SP 800-90A. I have only briefly reviewed some of the information released to date as a consequence of the FOIA request of Mr. A. Grayson.

I participated in three meetings: two conference calls on April 30 2014, and May 8, 2014 and I have dialed in to the physical meeting on May 29, 2014. Due to time limitations, it has not yet been possible to contact NIST with specific questions; I would like to take this step before finalizing this document.

This report assumes the reader is familiar with the technical background required to understand the NIST standards in the area of cryptography.

2 General observations on security standardization

The development of standard is a complex and delicate process with multiple stakeholders who often have conflicting interests. There are multiple tradeoffs:

- speed of development versus detailed scientific analysis;

- the selection of multiple schemes to satisfy specific needs versus a universal and perhaps simpler solution that is suboptimal for some scenarios;

- interoperability and backward compatibility: to which extent does one take into account existing deployments versus novel and improved schemes.

Developing security standards is typically more difficult than other standards. In order to select the most appropriate candidate(s) a functional or performance analysis is not sufficient; a method can only be included in a standard if it satisfies a minimum security level. However, establishing the security level can be very difficult for the following reasons:

- The security requirements depend on the threat environment; this environment may be different for each user, hence it may be very difficult to agree on the appropriate security definition.

- It is difficult to reduce the security level of a scheme to a single number; a single cryptanalytic attack is characterized by multiple parameters (computation, storage, memory accesses, number of chosen/known texts); very often several attacks need to be considered with different parameter sets. In addition, one should consider robustness against implementation flaws. These elements make it very hard to rank competing schemes.

- In the best case (typically for higher level schemes) the security of a scheme can be reduced with a reduction proof to the security of a building block or to the difficulty of a well-understood mathematical problem. The validity of a proof is always constrained to a model, that may or may not fit the environment in which the scheme will be deployed. Unfortunately these proofs can be very tricky to write and/or validate; it has happened that proofs were published and later shown to be erroneous. Moreover, it is still not the case that for all settings highly efficient constructions exist with a tight security reduction.

- For some building blocks (block ciphers, hash functions) the security level can only be established by intensive cryptanalysis performed by a large group of researchers. The security evidence consists of security

proofs against specific attacks in combination with the absence of a realistic attack; also relevant is the security margin compared to reduced variants that succumb to attacks.

A second aspect is that the security level of a scheme decreases with time. The reasons are the increase of computational power for cryptanalysis due to Moore's law and the improvement of algorithms for cryptanalysis (an example for the latter are the attacks on SHA and SHA-1 specified in FIPS 180). This implies that for each standard a plan is needed to review the standard on a regular basis and to withdraw the standard if needed. There should also be an emergency withdrawal procedure, that requires additional resources to monitor the recent developments and assess their impact. History has taught us that revising widely deployed applications is very difficult, as this has a very high cost for the industry. A third element that is different in security standards are the specific interests of law enforcement and national security services. They typically want to reduce the security level offered (e.g. the decision by the Director of the NSA to set the key length of the DES to 56 bits) or allowed access to key material through an escrow mechanism (FIPS 185, Escrowed Encryption Standard).

3 Observations on the standardization process and the role of NSA

Over the years, NIST has established a very strong track record in developing cryptographic standards. In many cases they have done an outstanding job, in particular when running the AES and SHA-3 competitions. But also in other areas the pragmatic approach of NIST has resulted in standards and guidelines that are highly relevant and useful by avoiding some of the pitfalls of the procedures of other standardization bodies. As a consequence, the benefit and impact of some NIST standards has gone well beyond the statutory responsibility of NIST to develop cryptographic standards and guidelines for protecting sensitive government information on non-national security systems. Several standards (such as the AES) have been used to protect classified data, but they have also become worldwide de facto standards. A strong point of the development process by NIST is that the threshold for experts to get involved is lower than in many other standardization bodies, the procedures are rather open and flexible (less formal), and NIST has

some technical expertise to make difficult decisions. However, some of these elements can also present risks.

The number of cryptographic documents published by NIST in the last 15 years is very large. NIST has been very responsive to demands by industry to standardize specific schemes. The number of proposed special publications may have created some level of fatigue with the cryptographic community, in the sense that most researchers lack the time and effort to follow what is happening with all the documents and schemes. As a consequence, some suboptimal decisions have been made and it is likely that some documents have received less community review than would be desirable. This is not the case for the open competitions that resulted in the selection of AES and SHA-3.

Several decisions made by NIST (or by its predecessor, the NBS) have resulted in a lack of confidence of the academic and industrial community in NIST. In the 1970s, there was a lack of transparency in the selection of the key length and the design criteria of the DES (FIPS 46). Even if it was obvious in the 1980s that the key length was no longer adequate, support for the DES was withdrawn only in 2004.[2] NIST also waited too long (until 1999) to publish the Triple DES (TDEA) standard in FIPS 46-3. A second example is the proposal of DSA as the digital signature standard in FIPS 186 (while RSA was the de facto industry standard). A third example is the publication of SHA, SHA-1 and the SHA-2 family in FIPS 180: these functions were designed by NSA and no information was provided on the design criteria or the security margin. Finally there is the publication of FIPS 185 (EES). However, the confidence of the community has NIST had increased in the past 15 years after the excellent work performed by NIST during the AES and SHA-3 competitions. Nevertheless, a number of decisions made by NIST were seen as controversial.

[2]Note that the briefing book states that by the mid 1990s DES was vulnerable to key exhaustion (page 10) and that the DES key search became practical by the mid 1990s (page 33). In 2013 NIST has decided that a security level of 80 bits is no longer adequate; if one applies Moore's law, one can extrapolate that a 56-bit key would have been adequate until 1977.

4 Comments on individual standards and guidelines

The previous section contains some brief comments on FIPS 180 and FIPS 185. There seem to be no concerns with the security of FIPS 197 and FIPS 198. Due to time limitations, I was not able to study in more detail the following special publications included in the NIST briefing book:[3]

- SP 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography
- SP 800-56B Recommendation for Pair-Wise Key Establishment Schemes: Using Integer Factorization Cryptography
- SP 800-56C Recommendation for Key Derivation through Extraction-then-Expansion
- SP 800-57 Recommendation for Key Management
- SP 800-106 Randomized Hashing for Digital Signatures
- SP 800-131A: Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
- SP 800-132: Recommendation for Password-Based Key Derivation Part 1: Storage Application
- SP 800-133: Recommendation for Cryptographic Key Generation
- SP 800-135: Recommendation for Existing Application-Specific Key Derivation Functions

There are no indications that there are shortcomings in these special publications, but some of these may require some additional review. I also did not have time to study the three symmetric schemes in SP 800-90A, but there are no indications that there would be a problem with these schemes.

[3] I also did not review any special publications not listed in the NIST briefing book.

4.1 Dual EC DRBG (SP 800-90A)[4]

In 1999 NIST started the work on random number generators in collaboration with ANSI. A first version was published in 2007, with subsequent revisions in 2008 and 2012.

There is no doubt that the inclusion of Dual EC DRBG in SP 800-90A was a serious mistake. In the meeting of May 28, 2014, NIST has provided a detailed analysis of their view of what went wrong in the process. The Dual EC DRBG mechanism was proposed by NSA and first standardized as ANSI X9.82 Part 3 inside the ANSI accredited committee for financial services X9, more specifically in subcommittee X9F, working group X9F1 (Tool Standards and Guidelines Group); due to organizational issues, the developments in this committee are not amenable to a broad public review. In 2005 the X9F1 committee members were aware of the fact that the standard offered the potential for a back door, i.e., a party could select the parameters P and Q in such a way that it would be possible for this party to recover the internal state and predict future outputs (one element of evidence is US patent 2007189527, Brown, Daniel R. L. & Vanstone, Scott A., "Elliptic curve random number generation" with priority date January 21, 2005; this patent mentions an "escrow key" and shows how to generate the parameters P and Q to avoid such a key). In August 2003, the ANSI X9.82 draft document was submitted to ISO/IEC JTC1/SC27/WG2 (resulting in a published ISO standard in 2005). In 2005 NIST started the development of SP 800-90A, a.o. to take into account FIPS 140 validation issues. The document was published in spite of serious technical issues (bias in the output, and risk for a back door) identified during the public consultation. It has also been pointed out that the bias in the output could have been reduced by reducing the number of output bits, but this would have made it much more difficult to exploit a potential back door; this interplay may be the reason why the bias issue was not addressed. In August 2007 the possible back door discussed inside ANSI X9.82 was the subject of a high profile presentation at the Crypto rump session; the goal of this presentation was to draw the attention of the cryptographic community to the problem. This presentation lead to further discussions, but ANSI X9F1 decided to not revise or withdraw Dual EC DRBG from X9.82 and NIST decided to not revise or withdraw SP 800-90A.

[4]This document was originally published as SP 800-90; subsequently it was planned to add parts 90B and 90C and this version was renamed 90A; parts B and C are still under development.

The main response to the risk of a back door in the standards was to allow the users to generate their own P and Q in a verifiable way. This option has several problems

- It exposes users to back doors inserted by vendors, as it is required that the alternative P and Q need to be *"hard-wired into its source code or hardware, as appropriate"*; a verifiable way to generate these parameters is included in ANSI X9.82; SP 800-90A contains a reference to this method but not the method itself, with may be a problem for validation.

- SP 800-90A contains a warning that discourages the use of alternative parameters: *"The security of* **Dual_EC_DRBG** *requires that the points P and Q be properly generated. To avoid using potentially weak points, the points specified in Appendix A.1* **should** *be used. However, an implementation may use different pairs of points, provided that they are verifiably random, as evidenced by the use of the procedure specified in Appendix A.2.1 below, and the self-test procedure in Appendix A.2.2."*

- FIPS 140-2 validation of an implementation requires that the original (likely compromised) P and Q values are implemented; this comment is also made on page 35 of the briefing book: *"were specified for validation purposes".* On Wikipedia it is claimed that OpenSSL uses the default parameters in order to get such a validation. NIST has confirmed that they are not aware of anyone who has asked for validation of different P and Q values. Note that such a validation would be requested to an evaluation lab (and not to NIST) and the lab may or may not inform NIST. Moreover, adding additional parameters would likely result in a delay of the validation process; note also that the status of such an additional validation would be slightly different.

The argument by NSA to defend the proposed parameters P and Q was *"the protection of the existing investment".* This argument is very weak, since interoperability is not a requirement for DRBG implementations. Hence one could easily allow other values of P and Q in the standard without breaking any existing implementations or their certification.

In the presentation given to the COV, NIST has identified the following reasons for this mistake:

- Misplaced trust by NIST in the NSA.
- Insularity and standard group dynamics that resulted in the ANSI X9F1 editing committee failing to resist the strong push by the NSA in spite of very critical comments from the outside; moreover, NIST was focusing more on the symmetric DRBGs which were owned by them (while Dual EC DRBG was owned by the NSA).
- Procedural weaknesses in which important issues were raised repeatedly but not properly documented and handled.

The explanations provided by NIST are plausible, but it seems that not all decisions in the standardization process of SP 800-90A are properly documented; moreover, we did not have access to the source documents. This means that it is impossible to decide whether this mistake involved in addition to clever manipulation of the standards processes by NSA also some form of pressure on the technical and/or management staff of NIST. It is also not clear whether there would be any traces of such pressure in documents.

Without access to the documents, it is also difficult to decide whether or not NIST has deliberately weakened Dual EC DRBG. In his answer to the letter by Mr. A. Grayson of January 28 2014, Mr. P. Gallagher writes

> "NIST would not deliberately weaken a cryptographic standard."

However, the letter of Mr. P. Gallagher does not answer the question in the letter by Mr. A. Grayson on the response of NIST to the notification of the concerns by experts (in February 2006); instead it describes the response in September 2013. The answer of NIST to the November 2007 column of Mr. B. Schneier in Wired is also evasive:

> "We have no evidence that anyone has, or will ever have, the "secret numbers" for the back door that were hypothesized by mathematicians Dan Shumov and Niels Ferguson."

An appropriate response would have been to investigate who has generated the parameters P and Q and to report this to the public (presumably this would also have resulted in multiple requests to immediately withdraw the standard). According to the presentation on May 28, 2014, NIST staff had asked this question in an exchange with Cygnacom on October 27, 2004 and received as answer that "NSA had told not to talk about it." At this stage

we can conclude that NIST has been negligent w.r.t. the security of SP 800-90A, but we have insufficient information to decide whether or not NIST was complicit in introducing a back door in this standard.

Additional information on the development of Dual EC DRBG can be found on Wikipedia (`http://en.wikipedia.org/wiki/Dual_EC_DRBG`). It would be useful to reconstruct the full history of the events based on the original documents; this would allow us to verify the description and analysis provided by NIST and to reconcile this with the information on Wikipedia. However, this would require a substantial effort as the development and revision process stretches over 17 years and three standardization bodies. Moreover, it is likely that these processes are not fully documented.

4.2 Modes of operation (SP 800-38 series)

Following the publication of FIPS 197 (AES) in 2001, NIST has published several special publications on modes of operation. Such a mode defines how a block cipher (such as DES, Triple DES or AES) can be used to achieve one or more specific security goals. Overall, it seems that NIST has been responsive to criticism in developing these modes (e.g. the withdrawal of the RMAC proposal that was recommended by NSA), but the set of modes that has been standardized leaves in our opinion room for improvement. The approach of NIST in this area has been pragmatic (following the industry developments), with as consequence that modes have been standardized that are not robust or that can only encrypt short data units; this is regrettable as in several cases technically preferable solutions were available. However, there is no indication of introducing back doors or very weak schemes.

4.2.1 SP 800-38B (CMAC)

CMAC is without any doubt a better design than RMAC and the selection of CMAC was clearly appropriate. Perhaps a simpler scheme would have been to use the ISO 9797-1 standard LMAC (CBC-MAC with a second key in the last encryption). NIST could have made a stronger recommendation to stop the financial sector from using a standardized key notification protocol in which the value $E_K(0)$ is being sent; this protocol is incompatible with most MAC algorithms based on block ciphers and definitely with CMAC (as the value $E_K(0)$ is an internal key in CMAC). Replacing $E_K(0)$ by $E_K(1)$ in CMAC would have offered a limited mitigation of this problem.

4.2.2 SP 800-38C (CCM)

This standard was developed for wireless security (IEEE 802.11) and submitted to NIST. The CCM mode was chosen over the EAX mode, that was *"arguably technically preferable"* (citation from the briefing book). The main motivation to standardize CCM seems to have been to support the work of IEEE 802.11.

4.2.3 SP 800-38D (Galois Counter Mode or GCM and GMAC)

The main reason for selecting GCM over more efficient schemes was the patent situation affecting schemes such as OCB and IAPM. There were clear reasons to prefer GCM over the competing CWC proposal. A disadvantage of GCM as specified in SP 800-38D is the vulnerability to nonce reuse (this weakness is also present in other scheme such as OCB). Overall, GCM is not a very robust standard; there are serious problems if part of the key bits leak, if the MAC result is truncated too much, or if the nonce is reused. The standard contains extensive warnings for these issues, but one can wonder whether it is wise to select standards that are so brittle. It should be pointed out that for 3G security, a variant of the GMAC scheme had been standardized where the internal key (the value denoted by H in SP 800-38D) is refreshed for every message. In software implementations refreshing H for every message would bring a serious performance penalty. However, in hardware implementations (or in software implementations on processors with hardware support such as Intel's PCLMULQD instruction) this performance overhead is very modest (one encryption per block). At Crypto 2012, Iwata et al. have shown that there are errors in the original security proof for GCM; fortunately they were able to fix the errors, but this also illustrates that more care could have been taken in developing the standard.

4.2.4 SP 800-38E (XTS-AES Mode)

The role of NIST seems to have been limited to endorsing the IEEE Std. 1619-2007. This standard is not freely available. One can wonder whether this scheme is useful given that NIST has decided to restrict the maximum size of the data units to 2^{20} AES blocks (16 Mbyte) for security reasons (this restriction is recommended by not required in the IEEE standard).

4.2.5 SP 800-38F (Methods for Key Wrapping)

This guideline contains ad hoc constructions designed by NSA. The designs are conservative and slow; more efficient constructions with security reductions exist that can achieve the same security goals and that are "preferable on technical grounds" (e.g., the SIV mode). The cryptographic community has been unable to come up with reasonable security assumptions for a reduction proof for the Key Wrap schemes; NIST has identified an attack with high complexity that does not undermine the practical security of the scheme. The main reason to stick to the older designs in SP 800-38F is backward compatibility of implementations.

4.3 FIPS 186 (Digital Signature Standard)

4.3.1 DSA

The decision to select DSA over RSA was not broadly supported by the cryptographic community. Its main advantage (for the government) seems to have been that – unlike RSA – DSA could not be used for encryption; it is hard to see any advantage in this for the users.

The DSA is also a brittle standard: even a small bias in the generation of random numbers for a signature results in leakage of the private signing key. It would have been possible to partially mitigate this problem by computing this random number by hashing the private signing key and the message. Moreover, it has been shown by Bleichenbacher in 2001 that the DRBG used in DSA (FIPS 186) was flawed. NIST has addressed this error very quickly (note that this issue is not described in the briefing book). One can speculate whether this flaw was a genuine flaw, or whether this flaw was also a back door, that may have been useful if users tried to use the DSA keys in a different scheme for encryption purposes (using the same key for signing and decryption was at the time a common practice).

4.3.2 NIST curves for elliptic curve cryptography

Some authors have criticized the NIST curves. However, most experts believe that the curves selected by NSA and standardized by NIST do not have a back door. In the interest of transparency, it would have been desirable that the algorithm and full source code for the generation of these curves would have been made public, so that experts can verify the selection

criteria and the outcome. Moreover, standardizing specific curves (i.e. the domain parameters) is a two-edged sword. One reason to select a standardized curve is that point counting algorithms (and thus the generation of good curves) used to be computationally intensive. Second, the use of standardized curves, that are generated by a party that can be trusted, allows for optimized implementations and makes it easier to achieve interoperability. However, the properties of discrete logarithm algorithms imply that the cost for additional discrete logarithms is very small; hence standardized curves lower the threshold for mass surveillance (in particular if the key sizes are chosen on the edge of what is feasible). NIST should consider the publication of a standard algorithm and corresponding software to generate additional elliptic curves and should consider to use this tool to also publish some new curves. Note that the same comment on additional discrete logarithms applies to logarithms in finite fields: the use of standardized primes has similar benefits and disadvantages.

5 Procedural issues

The publication of the NISTIR 7977 draft (NIST Cryptographic Standards and Guidelines Development Process) is a good step forward. It is strongly recommended that NIST develops this document further, taking into account the comments received. For example, it would be valuable to expand on the principles stated in the document: transparency, openness, technical merit, balance, integrity and continuous improvement; it is recommended to add "due process", "avoiding undue influence", "usability and robustness". The principle of transparency would require version control on all documents from an early stage, a full documentation of all decisions, and clear processes for the disposition of each and every comment received.

It is not clear how NIST takes decisions on creating new standards or on contributing to or adopting standards of other standardization bodies (such as ANSI, IEEE, IETF, and ISO). In view of the substantial effort on standardization in the area of security, coordination between the actors can be beneficial. However, NIST should also consider to which extent these collaborations undermine the core guiding principles of transparency and openness (several standardization bodies restrict access to technical discussions to members only; moreover, many charge a fee for access to the final standard).

NIST should establish transparent procedures and time scales on the maintenance and review of standards, including both periodic reviews and emergency procedures.

NIST is legally required to coordinate with NSA in order to avoid overlap (on security standards development for federal information systems under FISMA section 3453 Section 303 (b) (1).) In view of the extensive expertise of NSA in the area of cryptography, there is no doubt that NSA can offer very useful information and feedback to NIST for this purpose, but also for other work of NIST. However, it seems that NSA (with its dual role) seems to be prepared to weaken US government standards in order to facilitate its SIGINT role. This undermines the credibility of NIST and prevents NIST reaching its full potential in the area of cryptographic standards. In view of this, the interface between NSA and NIST and the role of the NSA should be made much more precise, requiring an update to the Memorandum of Understanding. At the very least, the terms "consult", "coordination" and "work closely" should be clarified. Ideally, NIST should no longer be required to coordinate with NSA. There should be a public record of each input or comment by NSA on standards or guidelines under development by NIST.

NIST should try to increase the use of open competitions; while they are expensive, they seem to offer the best guarantee to a broad evaluation and to achieve consensus in a transparent way. It is clear that this would not be feasible for all standards developed by NIST, but perhaps a lightweight variant of the AES/SHA-3 procedure can be conceived in some areas.

In order to fully play its role NIST needs to invest in a larger expertise in cryptography and NIST should reduce the number of new standards and guidelines it publishes. The increased expertise could be achieved through a combination of hiring additional experts in cryptography as permanent staff members and increasing the number of short term contracts for experts to perform critical evaluations in the specific domain of a document under development or review (following the CRYPTREC approach). NIST should also coordinate with similar agencies in other countries.

It would be helpful for NIST to establish a Scientific Advisory Board to review on a regular basis major technical and procedural decisions such as the development of a new standard or the selection of a specific scheme; this advisory board should consist of experts from the stakeholders. The reports and recommendations of the Scientific Advisory Board should be public.

6 Recommendations

1. NIST should be put in a position to independently develop the best cryptographic standards and guidelines to serve the US government but also the broader community. In view of this, NIST needs to revisit its MOU with NSA and perhaps with other agencies. The interfaces should be clarified, and all interactions should be public and documented.

2. NIST should establish a life cycle management procedure for all its standards and guidelines in order to arrive at a process that supports its core principles: transparency, openness, technical merit, balance, integrity, and continuous improvement, as well as due process, avoiding undue influence, and usability and robustness. This would require transparent decision processes on starting work in an area, choosing an approach to go forward, version management for all drafts from an early stage, detailed and individual dispositions for each and every comment received, a documentation of all design decisions, and procedures for regular revisions and emergency revisions.

3. NIST should establish a Scientific Advisory Board that should evaluate on a continuous basis all technical and procedural decisions in the area of cryptographic standards.

4. NIST should increase its human resources for the development and review of cryptographic standards and guidelines: more expert staff members are needed with an education in cryptography who can evaluate the technical merits of solutions. Moreover, NIST should consider to hire experts on a contractual basis to review its existing and draft standards and guidelines.

5. NIST should consider how its collaboration with other standards developing organizations can be continued while adhering to its basic principles; more in particular, NIST should verify whether the processes in the other organizations are compatible with its requirements for transparency and openness and with the need for open availability of standards and guidelines.

6. NIST should critically review all its standards and guidelines and evaluate whether it is necessary to withdraw some of them or to revise them in order to include schemes that are technically preferable.

7. NIST should complete the development of NISTIR 7977 (NIST Cryptographic Standards and Guidelines Development Process) by the end of 2014.

8. NIST should establish collaborations with its counterparts in other countries in order to coordinate the development of open cryptographic standards and guidelines.

9. NIST should consider establishing a licensing regime so that in exceptional cases it can include patented solutions in its standards and guidelines in a way that benefits all users.

10. NIST should consider to allow anonymous comments on its documents.

June 27, 2014

Dr. Roberto Padovani
Chairman, Subcommittee on Cybersecurity
Visiting Committee on Advanced Technology
National Institute of Standards and Technology

Re: Comments on the NIST Cryptographic Standards & Guidelines Development Process

Dear Dr. Padovani:

Thank you for the opportunity to provide feedback to the Visiting Committee on Advanced Technology (VCAT) in its review of NIST's standards and guidelines development process. The charge to the Committee of Visitors (COV) asks that we provide individual assessments in two areas: (1) the principles that should guide the standards and guidelines development effort, the processes for engaging the cryptographic community and communicating with stakeholders, and NIST's ability to fulfill its commitment to technical excellence; and (2) NIST's cryptographic materials, noting when they adhere to and diverge from those principles and processes.

This report will offer my comments in response to the charge. All comments are my own; they do not reflect the view of the COV as a whole or of Visa Inc. Since I am neither a cryptographer nor a technologist, I am in no position to evaluate the technical merit of the NIST's cryptographic materials. However, I have experience leading security efforts in an industry that respects and relies upon NIST standards in a variety of operating environments throughout the world. And I can bring to bear a level of expertise in the governance, risk and compliance field.

I should note that the COV review was limited in scope due to time and resource constraints. The primary documents I reviewed are: the draft NIST Cryptographic Standards and Guidelines Development Process published in NISTIR 7977, together with the public comments thereon; a "briefing book" describing at a high level NIST's cryptographic standards and guidelines and how they were developed; copies of the documents establishing the legal framework within which NIST operates (the Administrative Procedures Act, the Federal Information Security Management Act of 2002 and the Computer Security Act of 1987, OMB Circular A-119, and the Memorandum of Understanding between the NSA and NIST); a slide deck describing the development of the Dual EC Deterministic Random Bit Generator (Dual_EC_DRBG) in NIST's Special Publication 800-90 (SP 800-90); and several shorter slide decks describing the development of AES and SHA-3.

NIST staff provided copies of all materials requested by the COV and made themselves available to discuss the material and answer questions. Staff were at all times responsive and straightforward in their approach to the matters discussed. The COV did not, however, review any original documents, other than the legal documents. This includes the emails and documents being produced in response to FOIA requests, which were being gathered at the time of our review and were said to be voluminous.

* * * * * * * * *

As a preliminary matter, it is interesting to note that NIST was not originally created to serve as an independent standards organization for the world. Its mission is to provide standards, guidelines, tests, and metrics to protect the non-national-security information systems of the US government. Yet, due to its productivity and the quality of its work, NIST's output has been widely adopted and is now valued far beyond its primary audience. In today's interconnected world, the value of common standards and guidelines – particularly in the security area – cannot be overstated. When each country or region adopts its own standards, interoperability is destroyed, which in turn increases cost and can make it impossible to provide quality service across geographies. This is as true of a payment system as it is of telecommunications or the Internet. Although the damage to commercial companies is considerable, the impact is greater on countries and their citizens, who may suffer from balkanization, reduced economic growth, and greater socio-economic challenges.

The development and maintenance of globally accepted security standards is a significant benefit to the United States, as well as to the rest of the world. But since their value lies in their global acceptability, common standards must be – and must be seen as – trustworthy and impartial. Maintaining trust in the process by which they are created is therefore of the utmost importance.

This is why the questions raised in the Snowden documents released in September 2013 are of such concern, not only to cryptographers, but to the broader community that relies on the standards published by NIST. The allegation that NSA has, or had, a program designed to insert weaknesses into global cryptographic standards – weaknesses that it could later exploit in support of its SIGINT mission – calls into question the integrity, not only of the Dual_EC_DRBG included in SP 800-90, but of all the cryptographic standards developed by NIST. More specifically, the previously published criticisms of Dual_EC_DRBG take on a new significance when seen in the light of these revelations. Previous critiques had pointed out that the DRBG, which was provided by NSA, could have contained a "backdoor" enabling NSA to predict its outputs. Now there is evidence that NSA not only could have done so, but had a program explicitly designed to do so. Did NSA intentionally insert the weaknesses in order to provide itself with a backdoor? Why would NIST have allowed this? The troubling implication is that NIST itself could have been part of a scheme to insert a backdoor in its own published standard. Any such activity would compromise the integrity of NIST's work and raise serious concerns.

For entities seeking to restore confidence in a process whose integrity has been called into question, the first step is to address the immediate concern with urgency and impartiality. NIST seems to have done so. The Snowden stories broke in September 2013; by September 10, NIST had issued a Supplemental ITL Bulletin strongly recommending against the use of Dual_EC_DRBG pending resolution of security concerns. At the same time, NIST re-opened SP 800-90A as a draft for public comment. Ultimately, NIST concluded that it had been a mistake to include

Dual_EC_DRBG in SP 800-90 without adequate disclosure regarding its weaknesses. In April 2014, it removed Dual_EC_DRBG from the draft guidance, recommended that current users transition to one of the three remaining approved algorithms as quickly as possible, and provided a list of cryptographic modules that include Dual_EC_DRBG. Before implementing the revised guidance in final form, NIST has requested final public comment.

Having identified a serious error, the next steps are to determine how and why the error occurred, identify the root cause, and take action to prevent a recurrence. NIST has undertaken this task as well. As reported to the COV, NIST staff conducted an extensive review of the processes by which the Dual_EC_DRBG was developed, in order to reconstruct what happened. For the benefit of the COV, staff provided a "plain English" explanation of the issues with Dual_EC_DRBG, explaining why it should not have been included in X9.82 (from which SP800-90 was adopted), or in SP 800-90, in its current form.

The reconstruction of events showed that the issues with the DRBG had been identified several times – formally and informally – during the standards development process, and that they had been discussed and addressed at the time. NIST now concludes, however, that the steps taken to address the issues were less effective than they should have been, and that the team failed to take actions that, in the light of hindsight, clearly should have been taken. The root causes of the failure were identified as trust in the technical expertise provided by NSA, excessive reliance on an insular community that was somewhat impervious to external feedback, group dynamics within the standards development team, and informal recordkeeping over the course of a multi-year development process.

The COV's review was not deep enough to evaluate these conclusions with certainty. However, all indications are that the reconstruction of events was done in good faith in a genuine attempt to understand the problem and develop solutions. NIST staff was forthcoming, direct, and self-critical in response to the COV's questions and provided all information requested. Although we cannot rule out other explanations, the ones provided by the internal review are plausible, given the nature of the group and the absence of formal procedure or documentation.

Having diagnosed the problem, NIST is now proposing actions to prevent a recurrence. The proposal is to formalize and make public the principles that guide the standards development process. As published for comment in NISTIR 7977, the principles are: transparency, openness, technical merit, balance, integrity, and continuous improvement. Are these the right principles? I believe they are. However, there are issues lurking within the principles that could cause problems when they are applied in practice. Below I offer recommendations to strengthen the principles and the process.

1. In General. The current draft of NISTIR 7977 seems intended simply to memorialize the principles under which NIST is and has been operating. There is no indication that anything was problematic or has been changed. This would seem an insufficient

response to the acknowledged weaknesses that led to the inclusion of the Dual_EC_DRBG in SP 800-90. **To demonstrate that it is practicing as well as stating its commitment to transparency and continuous improvement, NIST should acknowledge in its final Standards and Guidelines Development Process, or in an introductory document, that it has identified improvements to its processes and call out what those improvements are.**

2. Transparency and Openness. In general, these principles provide excellent safeguards against error. However, as NIST's internal review concludes, the protection they offer can fail when insularity and group dynamics lead decision makers to discount external inputs and place undue reliance on trusted insiders. In addition, the principles state only that NIST "strives" to be transparent and to maintain an open process. There is useful detail about how this is done in the Public Review and Outreach section, but it is rather generic and speaks most specifically to the Federal Information Processing Standards (FIPS).

   To build confidence in the process, the *principles* of openness and transparency should be reinforced with *process disciplines* designed to ensure continuous *awareness* of the risks to objectivity within a small community of technical experts. I believe the community benefits from NIST's informal, pragmatic approach to standards development and that considerable flexibility should be maintained. Within that context, however, I would recommend that an adequate level of process – without unnecessary bureaucracy – should be adopted, including the following:

   - **NIST should publish formal, repeatable governance procedures that stakeholders can expect and rely on in the development of important or complex standards and guidelines.** Other standards developing organizations typically maintain written procedures of this kind, at varying levels of detail. The procedures should, for example, set forth the criteria by which NIST decides which development mechanism to use (e.g., contest, adoption of existing standards, development of new standards) as well as the process for ensuring transparency and openness within each mechanism.

     The FIPS standards, which are developed using the protocols of the Administrative Procedure Act, may not require additional detail. Similarly, the existing description of cryptographic competitions is quite detailed and could easily be refined into a more prescriptive procedure. NISTIR 7977 is less clear on how NIST goes about adopting existing standards and developing new ones. There is an opportunity to clarify how these processes will be managed: for example, with public notice at certain points in the process, public comment periods, a process for submitting formal comments, and a description of how

decisions are made. As a further safeguard against error, the process could include an opportunity for "second review," within NIST or by independent experts as the situation warrants. However, I would not recommend an appeal process to higher levels of the US government, unless all those involved share NIST's mission devoted exclusively to technical merit and impartiality.

- **NIST procedures should require that records of the development process be maintained in a systematic and reliable way.** Something as simple as a "project file" with a single point of accountability would make it easier to track the issues that are raised, by whom, when, and how resolved, over a multi-year development cycle. When adopting standards developed by other organizations, NIST should obtain and review similar files from the developing organization, in order to validate that that organization followed processes commensurate with NIST principles before putting its own imprimatur on the end product.

- I would also suggest that **in those processes where formal comments are submitted, the comments should be tracked and their dispositions recorded, at least internally within NIST. For complex or long-running development processes, a quality review of the dispositions should be performed prior to final publication.** There are tools available to manage this type of recordkeeping in order to keep administrative burden to a minimum.

- The volume of material now being produced by NIST may make it unrealistic to suppose that the external community will have the time, interest, and resources to provide adequate review of all the material published for comment. To address this, **NIST should consider requiring a paid independent review of certain types of proposals, for example those involving heightened levels of complexity or importance, or those containing significant elements whose provenance might be questioned.**

3. Technical Merit and Balance. These two principles address the critical question of the basis on which NIST makes its decisions. When applied over time in an environment of transparency and openness that allows the community to judge the process and its outcomes, these principles should dispel concerns that decisions are being made on extraneous, improper, or secret grounds. In saying that decisions are based on "technical merit," NIST makes a strong commitment to the pursuit of excellence without regard to any competing or conflicting interests of the United States government or of any other party. But confusion is introduced by the discussion of "balance," which seems to indicate that almost any consideration relevant to the needs or interests of stakeholders – including the US government – could be considered. This tension could be resolved in several ways. My recommendation would be that:

- **NIST should clarify that "technical merit" is first and foremost a question of security, but that it also incorporates the considerations of efficiency, interoperability, and practical implementation that are currently mentioned under the principle of "balance."** NIST should also emphasize that in making its decisions based on technical merit, it specifically does *not* weigh or balance interests of stakeholders that do not bear on the security, efficiency, interoperability, or practical implementation of the solutions it is considering.

- **NIST should clarify the principle of "balance" to ensure that it is not misunderstood as including considerations that fall outside of, or conflict with, its mission.**

4. Integrity. This principle is important and well stated. I believe, however, that it is somewhat incomplete and would benefit from an explicit acknowledgement of the risks that arise from potentially conflicting interests. This is typical in corporate codes of conduct, for example, and seems appropriate in light of current and historical concerns over the relationship between NIST and NSA. Participants in the development process should understand that the risk from conflicts of interest arises from the *appearance of impropriety,* even in the absence of actual misconduct.

   For example, the mere existence of NSA's dual mission – both to develop security standards and to gather intelligence (including by intercepting signals potentially secured by those same standards) – creates an appearance of impropriety regardless of whether any misconduct ever occurs. I understand that NSA may be contemplating some form of segregation of duties that would mitigate this inherent conflict. Unless and until that occurs, and given the requirement that NIST consult with NSA when developing standards, the appearance of conflict will remain as an inherent risk in the standards development process. Other participants could have potential conflicts as well, including commercial entities with interests in proprietary technologies. To address this issue, I would recommend that:

   - **The integrity principle should include a reference to the importance of avoiding – or appropriately managing – conflicts of interest in the standards development process, and NIST should adopt procedures to manage the risk presented by those conflicts.** Without regard to legal requirements, it will likely remain valuable for NIST to consult informally with potentially conflicted participants, such as NSA, in order to obtain their expertise. Some form of internal control should be instituted over these interactions. One possibility would be to require affirmative security proofs, where feasible, in situations involving potential conflicts. NIST could also consider procedural safeguards

commonly used in other contexts. For example, NIST could require that participation by potentially conflicted parties be recorded in the project file, that the provenance of contributions from those participants be disclosed, that significant comments from those participants be submitted formally, that their submissions be given a second level or independent review, and/or that they be excluded from final decisions regarding elements they have contributed. In the case of Dual_EC_DRBG in SP 800-90, those evaluating its weaknesses would probably have taken more aggressive measures to disclose its provenance and recommend usage, had they been following established procedures for addressing the potential conflicting interests of the NSA.

In addition, the "integrity" principle alone may be insufficient to address the risks from insularity and group dynamics identified in the staff review of SP 800-90. Given the nature of cryptographic work, it would seem these risks are likely to recur. To combat this, I would recommend that:

- **NIST should adopt a program of leadership, training, and communication that reinforces a culture of openness and impartiality.** Among other things, the program should be designed to ensure that staff gives even-handed consideration to outside feedback and uses formal processes to avoid "group think" and undue reliance on long-term colleagues and friends.

5. Continuous Improvement. This principle is important and well stated. As noted under "Transparency and Openness," I would suggest that formal comments involving identified vulnerabilities be tracked and dispositioned within a project management file or system maintained internally at NIST. In addition, in the spirit of continuous improvement, I would recommend that:

   - **NIST should conduct a periodic review of its Standards and Guidelines Development Process, as needed but at least once every five years.**

The final element of the charge to the COV is to assess NIST's cryptographic materials, noting when they adhere to and diverge from those principles and processes. It is clear that the cryptographic materials developed through cryptographic competitions adhere quite rigorously to the principles, and they have in general been warmly received by the community of cryptographers and standards users. As to the remaining cryptographic materials, I do not believe the COV has had sufficient opportunity to draw meaningful conclusions about their development. I do agree, however, that in order to restore and maintain trust and confidence **NIST should complete the planned review of its cryptographic materials – not only for adherence to the principles, but also to ensure that the root causes of the errors identified in the adoption of the SP 80-900 do not taint those standards as well. Should any errors or**

defects be identified in other materials, it will be important for NIST to take prompt, public action to remediate the issues.

Thank you again for the opportunity to provide this report.

Sincerely,

Ellen Richey

Summary of Recommendations

1. To demonstrate that it is practicing as well as stating its commitment to transparency and continuous improvement, NIST should acknowledge in its Standards and Guidelines Development Process, or in an introductory document, that it has identified improvements to its processes and call out what those improvements are.

2. NIST should publish formal, repeatable governance procedures that stakeholders can expect and rely on in the development of important or complex standards and guidelines.

3. NIST procedures should require that records of the development process be maintained in a systematic, reliable, and transparent way.

4. In those processes where formal comments are submitted, they should be tracked and their dispositions recorded, at least internally within NIST. For complex or long-running development processes, a quality review of the dispositions should be performed prior to final publication.

5. NIST should consider requiring a paid independent review of certain types of proposals, for example those involving heightened levels of complexity or importance, or those containing significant elements whose provenance might be questioned.

6. NIST should clarify that "technical merit" is first and foremost a question of security, but that it also incorporates the considerations of efficiency, interoperability, and practical implementation that are currently mentioned under the principle of "balance."

7. NIST should clarify the principle of "balance" to ensure that it is not misunderstood as including considerations that fall outside of, or conflict with, its mission.

8. The integrity principle should include a reference to the importance of avoiding – or appropriately managing – conflicts of interest in the standards development process, and NIST should adopt procedures to manage the risk presented by those conflicts.

9. NIST should adopt a program of leadership, training, and communication that reinforces a culture of openness and impartiality.

10. NIST should conduct a periodic review of its Standards and Guidelines Development Process, as needed but at least once every five years.

11. NIST should complete the planned review of its cryptographic materials – not only for adherence to the principles, but also to ensure that the root causes of the errors identified in the adoption of the SP 80-900 do not taint those standards as well. Should any errors or defects be identified in other materials, it will be important for NIST to take prompt, public action to remediate the issues.

From: Ronald L. Rivest
Vannevar Bush Professor
Massachusetts Institute of Technology
Cambridge, MA 02139
To: Visiting Committee on Advanced Technology (VCAT)
National Institute of Standards and Technology (NIST)
Gaithersburg, Maryland
Re: Preliminary findings regarding NIST's development of cryptographic standards
Date: May 30, 2014

This note conveys my preliminary findings, observations, and suggestions in response to the charge (dated 4/24/14) conveyed to me as one of the Committee of Visitors (CoV) serving the Visiting Committee on Advanced Technology (VCAT), advisory to NIST, with respect to the NIST's process for developing cryptographic standards.

As requested, these findings are my personal findings, and are not the result of any consensus or other deliberative process with others. They are based on the (excellent) materials and presentations provided by NIST, as well as my own background and experience with cryptography and cryptographic standards. They are not based on materials that are subject to FOIA requests to NIST, since these materials were unavailable. These findings are also quite limited, due to the very brief time available for their preparation.

I. Context

The present review was stimulated by the revelation that the NSA may have engineered a “back-door" into the NIST standard Dual-EC-DRBG for generating (pseudo)random numbers, which might enable the NSA to read encrypted traffic when the Dual-EC-DRBG was used to generate keys and/or other cryptographic parameters.

While the actual damage caused by such a back-door to users of NIST cryptographic standards may be small (few users may have used Dual-EC-DRBG), the damage to NIST and its credibility for developing trustworthy cryptographic standards is considerable. Not only do other NIST standards developed in coordination with the NSA now need critical review, but the process for developing future standards needs re-assessment and reformulation.

The most salient aspect of the necessary review is the past and future reliance of NIST on the NSA for cryptographic expertise.

A secondary aspect is to assess whether NIST's cryptographic standards process provides adequate robustness should an existing standard become broken. Cryptographic algorithms are subject to catastrophic failure if and when a new attack is developed, rendering all fielded implementations of that algorithm insecure. A well-studied alternative standard must be available.

II. Review and Assessment

This section (a) reviews NIST's process for developing cryptographic standards, and (b) discusses some of the particular cryptographic standards. Due to the short time-frame available for producing this

report, these analyses of particular standards are quite limited, and further work is warranted.

II.A. Process

The NIST process for developing cryptographic standards has by-and-large been a good one. In particular, the process for developing AES was particularly open and successful in the engaging the world-wide cryptographic community.

Cryptographic standards are by their nature quite unusual. They not only provide for interoperability, perhaps by codifying existing practice, but also provide assurance that they will withstand severe adversarial attack. Details matter enormously, and the assessment of the cryptographic strength of a proposed standard requires very substantial effort and a great deal of expertise. Even so, methods believed to be secure may sometimes fall to a novel attack.

Indeed, it is very important for NIST to maintain a standards-development strategy that is robust in face of failure of a cryptographic standard or the failure of a cryptographic assumption underlying the security of an adopted standard. The situation NIST is currently addressing (having to withdraw a standard because it is no longer deemed to meet the desired security objectives) should not be expected to be a unique occurrence. Indeed, NIST has had similar issues arise before with the development of secure hash algorithms. Cryptography is delicate and fragile, and sometimes gets broken. NIST should expect and be prepared for events of substantially greater severity than the current situation.

Such a robust standards-development strategy should include the development of alternative approved methods for accomplishing any given security objective. Moreover, NIST should encourage implementors and users of their standards to implement more than one, with a facility for easy switching between them. Just as your car has a braking system and also has an emergency braking system, one's crypto implementation should have a built-in backup for each functionality.

Internally, NIST has very limited cryptographic expertise: just a handful of cryptographers. The internal capabilities at NIST to develop and evaluate cryptographic standards is by itself not sufficient to produce the desired cryptographic standards, particularly given the number of standards and guidelines involved. Additional expertise is essential.

NIST has three available external sources for obtaining the requistite effort and expertise: the NSA, industry, and academia.

The NSA has the world's largest collection of cryptographers, and has an enormous body of experience and expertise. On the basis of pure technical ability, they should certainly be at the top of anyone's list of advisors for the development of cryptographic standards.

However, the NSA has dual obligations: one to provide intelligence, and one to assist in protecting the U.S. national information infrastructure. These may be in conflict: the development of good cryptographic standards may negatively affect intelligence operations while benefitting the security of our national information infrastructure.

However, cryptographic standards may appear to provide a means of advancing both of NSA's objectives, if the standard was one that “only NSA could break,” and if having a standard that “only NSA could break” was viewed as an acceptable trade-off in return for having NSA's advice on its

construction.

Politics requires, however, that such an approach not be achieved by stealth, but rather by explicit approval through a democratic political process, backed by widespread popular approval. In fact, such popular approval does not now (and probably will never) exist, and there is really no chance that explicitly giving the NSA (or more broadly, the government) unfettered access to encrypted data through a back-doored standard would meet with democratic political approval.

Recent revelations and technical review support the hypothesis that, nonetheless, the NSA has been caught with ``its hands in the cookie jar'' with respect to the development of the Dual-EC-DRBG standard. It seems highly likely that this standard was designed by the NSA to explicitly leak users' key information to the NSA (and to no one else).

The Dual-EC-DRBG standard apparently (and I would suggest, almost certainly) contains a ``back-door'' enabling the NSA to have surreptitious access. The back-door is somewhat clever in that the standard is not designed to be “weak" (enabling other foreign adversaries to perhaps exploit the weakness as well) but ``custom'' (only the creator (NSA) of the magical P,Q parameters in the standard will have such access). Of course, the ability to restrict access to NSA only supposes that NSA can keep secret its knowledge of the P/Q relationship, and that no adversary can compute the secret P/Q relationship.

Apparently the “intel” side of NSA has tried to “slip one by” the standards bodies (ANSI and NIST), in order to have a standard that the NSA could compromise. This compromised standard hearkens back to the debate in the 90's about “key escrow” and the “Clipper chip”, when the government proposed standards that would explicitly provide government access to encrypted data. These proposed standards were widely rejected on both technical and political grounds.

Today, NIST should not be developing or promoting standards that would provide government the technical means to access encrypted data, or that would enable the government to otherwise defeat the security objectives of cryptographic standards.

The current review of NIST's processes and procedures, in the wake of the Dual-EC-DRBG bungle, are quite appropriate and welcome. NIST needs to re-address the question of how it obtains the necessary cryptographic effort and expertise in the development of its cryptographic standards, since the NSA no longer appears to be a fully trustworthy partner, in spite of its tremendous technical competence in the field.

An initial question is naturally: What other standards have been ``tainted'' by NSA's involvement? Are there other existing standards or cryptographic parameters that should now be suspect, having been developed in coordination with the NSA, or even developed wholly by the NSA? Are there other standards that, like Dual-EC-DRBG, could give the NSA an advantage over its users? Fortunately, the Dual-EC-DRBG is now being withdrawn as a standard. Should others be withdrawn?

I provide some initial thoughts on particular existing standards in the following section. But these are only initial thoughts; NIST should begin a longer-term process of review and (when appropriate) replacement.

Going forward NIST should also greatly expand its cryptographic competence, by hiring more cryptographers. The cryptographic standards developed by NIST are critically important, and NIST

needs substantially more in-house expertise for the development, promulgation, and continuing review of these standards.

II. B. Particular standards

NIST provided a list of standards that may merit special consideration; some were either developed entirely by the NSA, or had substantial NSA involvement in their development.

NIST identified 5 FIPS and 19 Special Publications in their “Briefing Book” to the CoV as having had an interesting or potentially problematic development history (perhaps due to the large role played by the NSA in development). I provide comments on some of these below.

FIPS 180 (Secure Hash Standard)
This standard is interesting in part because the original NSA-developed standard was apparently flawed, and had to be tweaked (thus going from SHA-0 to SHA-1). The technical rationale for the tweak was never released by the NSA (and it isn't clear if any NIST staff ever knew the technical rationale for this change). This work is now augmented by the alternative SHA-3 standard (Keccak), developed by Europeans as part of a NIST-sponsored competition. It is good to see this sort of redundancy and robustness in the suite of available standards.

FIPS 185 (Escrowed Encryption Standard)
This standard was a double failure: it had little political support, and it was viewed as technically flawed. It illustrates the problem of trying to solve what are essentially political problems by technical fiat, which just doesn't work.

FIPS 186 (Digital Signature Standard)
The original standard was developed by the NSA, but contains no ``magic constants'' or other parameters that could hide a backdoor. My biggest concern with this standard is that it is subject to catastrophic failure (including loss of the signer's private signing key) if the signer's random-number generator is flawed. This sort of vulnerability is unnecessary in a digital signature standard.
The extension in 186-2 (ECDSA: Elliptic Curve Digital Signature Standard) introduces a variant with the same catastrophic failure vulnerability. Furthermore, the ECDSA standard specifies a set of elliptic curves for use with this standard. These curves, as noted by NIST, have unclear provenance (they came from the NSA, but were unjustified choices). Perhaps they hide a backdoor. Moreover, there is little reason why an ECDSA signature standard needs to specify the curves at all, when the signer could choose his own curve(s).

FIPS 197 (Advanced Encryption Standard)
This standard is perhaps the jewel in the suite of NIST cryptographic standards. It was developed in a very open, transparent process, including an international competition.

FIPS 198 (HMAC key hash message authentication code)
This standard is a good example of adopting a standard from another organization (IETF). The HMAC construction comes with a security proof (the message authentication code is unforgeable if the hash function from which it is built satisfies certain properties), which may explain its lack of controversy and smooth adoption history, and illustrates the virtues of standardizing on provably secure cryptographic constructions.

SP 800-38 series A—F (block cipher modes of operation)
These standards are classic cryptographic material; their development illustrates good dialogue between NIST, academia, and industry. In general, the approved modes are accompanied with security proofs, which is critically important. One notable exception is 38F (key-wrapping); a provably secure alternative standard should also be developed and adopted.

SP 800-56 series A—C (Pairwise key establishment methods AB and key derivation C)
These standards (A,B) were developed by a team consisting of NIST and NSA personnel. It illustrates well perhaps the lack of adequate cryptographic staff at NIST, as these are standards which should easily have been developed by NIST staff, with at most a review by the NSA.

SP 800-57 (Key management guidance)
Cryptography is hard to use correctly, and so it is good to see NIST working to improve the security engineer's understanding of the broader issues surrounding cryptography, such as key management. Indeed, the federal government should do much more to improve the available documentation, educational materials, and guidance regarding the use of cryptography.

SP 800-67 (TDEA)
No comment on this standardization of a legacy mode of operation.

SP 800-90A (Deterministic Random Bit Generators)
The smoking gun. The appropriate NIST process is already underway to remove the Dual-EC-DRBG from this standard, as it appears almost certain that this standard contains a backdoor accessible to the NSA. We see here the wisdom of having a number of alternative standards for a given cryptographic objective: when one fails or becomes unsuitable, there are natural alternatives to fall back on. (A minor note: I do think NIST does a substantial dis-service by not sticking to standard terminology; these generators are *pseudorandom* and not *random*. This field is hard enough without the added confusion caused by abusing terminology.)

SP 800-106 (Randomized Hashing for Digital Signatures)
No comments.

SP 800-108 (Key Derivation using pseudorandom functions)
No comments.

SP 800-131A (Transitioning to better algorithms and longer keys)
Excellent.

SP 800-132 (Password-based key derivation for storage applications)
No comments.

SP 800-133 (Cryptographic Key Generation)
No comments.

SP 800-135 (Existing Application-specific key derivation functions)
The question raised by this standard really is “Why is NIST bothering to standardize these existing industry standards?” Perhaps there is a government need, but it isn't obvious to me.

III. Recommendations

I would like to make the following recommendations and suggestions to VCAT to consider, as to how NIST might improve its processes and procedures.

1. **NIST should hire more cryptographers.**
   To develop, evolve, maintain, and improve its suite of cryptographic standards, NIST should greatly expand its staffing in the area of cryptography. All the more so since NIST can no longer rely so naively on guidance from the NSA. I would suggest that, at minimum, NIST hire at least two cryptographers for each cryptographic standard that it has approved or is considering. (That is not to suggest that each cryptographer works only on one standard, but that this ratio of staff of number of standards seems a good baseline starting point.) A team of 40 or so cryptographers might be a good initial staffing goal.

2. **NIST should ask the NSA for full disclosure regarding all existing standards.**
   NIST (and the public) should know whether there are any other current NIST cryptographic standards that would not be acceptable as standards if everyone knew what the NSA knows about them. These standards should be identified and scheduled for early replacement. If NSA refuses to answer such an inquiry, then any standard developed with significant NSA input should be assumed to be “tainted," unless it possesses a verifiable proof of security acceptable to the larger cryptographic community. Such tainted standards should be scheduled for early replacement.

3. **NIST should restructure its working relationship with NSA.**
   NIST should work to ensure that the NSA is not able to exert undue influence on the development of standards; NIST's reliance on NSA's expertise should be greatly reduced. All standards-related communications between NIST and the NSA should be in writing and part of the public record. NIST should not approve a standard just because the NSA says that it is in use and deserves standardization. The politics of restructuring this relationship may be complex, but NIST needs somehow to make itself *much* less dependent on the NSA for any cryptographic expertise.

4. **NIST should develop and implement a plan to increase involvement by academia and industry in the standards-development process.**
   While NIST has been very successful at engaging academic and industry in some portions of the standards process (as with AES), I belive that many other standards efforts have been ``below the radar'' and received scant attention from academia and industry. An increased effort from these quarters is needed to counterbalance an expected decreased reliance on the NSA.

5. **NIST should publicly commit to developing and promulgating only standards that are ``best of breed'' and that are not tainted by the needs of the**

intelligence community.

Any perception that NIST is being manipulated to serve the intelligence needs of the NSA will result in a total collapse of NIST cryptographic standards process, as it will lose all credibility.

6. **NIST should replace the specified ECDSA elliptic curves with guidance to users on how to choose their own elliptic curves securely.**

   It isn't clear why the ECDSA standard should specify particular curves at all. While there may be patent issues involved with using elliptic curves, such issues should be unchanged whether the standard specifies particular curves, or merely provides recommendations on how to choose curves securely. It is possible that the specified curves contain a backdoor somehow. It is also possible that the specified curves are in fact quite secure and are excellent choices. Given the current situation, however, it seems prudent to assume the worst and transition away from the specified curves.

7. **NIST should emphasize the adoption of cryptographic standards with provable security properties.**

   Phase out standards whose security properties are unproven in favor of those whose security standards are provable under reasonable assumptions. At least, a provably secure alternative should be available among the NIST standards for a given application. For example, NIST should develop and adopt a provably secure key-wrapping standard.

8. **NIST should ensure that each cryptographic objective is attainable in more than one standardized way, and that among such alternatives there is at least one that is publicly available and royalty-free.**

   Standards bodies that require payment to see published standards and standards that are not royalty-free may inhibit adoption of effective cryptographic techniques. The alternatives for a given cryptographic objective should be based on dissimilar assumptions, so that they are not likely to be broken with a common attack.

9. **NIST should strengthen its efforts to make its cryptographic standards understandable and more easily usable by security engineers.**

   Cryptography is complex; it is easy to mis-use and unintentionally and unknowingly lose the desired security properties. NIST should expand its suite of educational materials, including more descriptive use-cases. NIST should also work to minimize hazards by assessing cryptographic API's and identifying insecure defaults.

10. **NIST should take a broader and longer-term view.**

    The cryptographic standards developed by NIST have substantial impact on the use of cryptography world-wide, and will be in-use for decades. NIST should work to see that its charter mandates a broader, longer-term view. Cryptographic standards should be expected to have a life-cycle (sometimes with an abrupt end), to need continuing review, and to expire unless renewed by a given date. The efforts of NIST to involve the world cryptographic community in the development of its standards is laudable and should continue.

To: **Roberto Padovani, Chair, VCAT Subcommittee on Cybersecurity**

From: **Fran Schrotter, Sr. VP & COO, ANSI, and member of the COV**

Date: **June 6, 2014**

Subject: Individual assessment of NIST's current cryptographic standards and guidelines development processes

I would like to begin by thanking the NIST Visiting Committee on Advanced Technology (VCAT) for the opportunity to participate as a member of the Committee of Visitors that was formed to serve as technical experts to assess NIST cryptographic standards and guidelines development process and, if necessary, to provide findings on how it can be improved.

First and foremost, I would like to commend NIST for the extraordinary job that they have done in providing the Committee of Visitors (COV) with total transparency into the processes by which NIST develops cryptographic standards and guidelines. At its first meeting, the COV was provided a full explanation of the concerns that led to the formation of the COV and the steps that had already been taken within NIST to address these concerns. The COV was provided with very detailed information regarding NIST's role in the development of cryptographic standards and guidelines, including its relationship with the NSA. As the COV engaged in its deliberations, each and every request for more background documentation and additional information was met promptly and thoroughly by NIST staff. They went above and beyond to ensure that the COV was provided with very detailed factual information even when that factual information may have pointed to shortcomings in the NIST process.

While a number of changes have already been made, NIST has demonstrated that it is fully committed to considering any additional changes to their processes that would result in a more robust system overall – one that adheres fully to the principles of transparency, openness, technical merit, balance, and integrity.

Having thoroughly examined all of the documentation that was provided to me as a member of the COV – in particular as it relates to the processes for the development of NIST cryptographic standards and guidelines – I submit the following individual assessment. My comments are directly influenced by many years of active engagement in the private-sector voluntary consensus standardization system, both nationally and internationally.

Process-based Characteristics – Feedback on the Principles that Should Drive NIST Standards Development

To the extent that NIST's objectives can be addressed through voluntary consensus standards developed in the private sector, the guidance established in OMB Circular A-119[1] should prevail. Where an alternative process is more compatible with its goals, NIST should make this known to the public and explain the basis for the chosen path or the departures from its published process. Such clarifications will allow the public and stakeholders to understand the degree to which they may participate as well as manage their expectations throughout.

Documentation of fair rules in the form of written and publicly available procedures, coupled with consistent implementation of applicable procedures, is key to ensuring that stakeholders understand the goals and limitations of a standards development effort and the ways in which they can participate.

Written Procedures and Summary of Deliverables

NISTIR 7977 *NIST Cryptographic Standards and Guidelines Development Process (Draft)* is a good basis upon which to build a more detailed and expanded set of rules for internal and external use with respect to documents within the purview of the Computer Security Division (CSD). The next version could further demonstrate NIST's recognized commitment to fairness and public engagement, which is evidenced by the diversity of outreach, competitions, and opportunities for participation described briefly in NISTIR 7977.

NIST should further clarify its roles: 1) as a developer of standards and guidelines under FISMA for use in U.S. federal non-national security information systems; and 2) as a technical contributor/stakeholder in connection with voluntary, global standards development. NIST should also address how these roles play out in relation to any ongoing obligation to consult with NSA or any other government agency.

For ease of reference, a matrix or graphic summarizing the types of deliverables issued by CSD, including the document type, key rules, limitations, and purpose, could serve as a helpful reference document internally and for the public. As well, consistent training of staff in accordance with written procedures and policies would help to ensure that NIST's goals are achieved through fair and appropriate processes.

Criteria Applicable to Each Deliverable

- **Openness:**
  - The nature of the deliverable, as broadly addressed in the section entitled *NIST Publications*, should be further defined. This description should also address the criteria that will determine where NIST's role as a standards developer ends and when or if it is expected that the document will be transitioned to another standards developer for completion or maintenance.
  - The degree to which the development or approval process is open to public input or whether the process is invitation-only or a NIST-only process, etc., should be clear.
  - If NIST is required to consult with another organization, then that should be noted.

[1] *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.* http://www.whitehouse.gov/omb/circulars_a119

- Requirements for public notice should be documented, including both fixed and flexible aspects of the process. For example, all standards are announced for public comment; however, type A requires a 60-day comment period, while 30-60 days may be used for type B.
- Key decision-making points in the development and approval process should be clear.
- Identify internal and external decision makers – including a source for their names and affiliations as well as the identification of any other opportunities through which the content of the document may be influenced. For example, clarify who decides which type of document will be developed, how decision-makers are appointed, and what the rules are for finalizing such a decision, e.g., approval of a document.

- **Balance of Interests**
  - How balance is defined by type of document should be known. The degree to which a balance of interests of stakeholders will be sought and the mechanisms (routine and other) that will be utilized to engage participants should be identified.
  - The interest categories relevant to the standard should be discreetly defined and those participating in the process, other than through public input, should be assigned or select an interest category. This will demonstrate a representation of interests in the decision-making process.

- **Safeguards against Dominance**
  - Safeguards against dominance should exist. Dominance may be defined as the position or exercise of dominant authority, leadership, or influence by reason of superior leverage, strength, or representation to the exclusion of fair and equitable consideration of other viewpoints. Written and published procedures as well as identification of participants and decision-makers at key phases help guard against situations in which dominance can occur.

- **Approval Decisions or Actions**
  - Voting requirements should be identified when they apply.
  - Absent a voting requirement, there should be clear and documented rules for determining the basis upon which a decision to proceed is made.

- **Public Input**
  - The process by which public input will be received, considered and responded to (or not) should be documented. It may vary by document type, but the process and any limitations should be known.
  - All comments should be submitted in writing. Given the nature of the documents and the need perhaps to protect proprietary information, comments could be shared without attribution.

- **Policies**
  - Rules that address key policy considerations should be documented, such as: the use of patented technology in standards; guidance on commercial terms and conditions within standards; publication and maintenance cycles; and the development and issuance of interpretations.
  - A written interpretations policy should exist, including whether interpretations will be issued and if so, by whom and how.

- **Continuous Improvement**
  - As NIST notes its goal of continuous improvement, it is also important to establish a maintenance cycle to keep documents up to date. For example, some documents may be open for review continuously while others may be reviewed on a 3-5 year cycle.

- **Neutral Oversight**
  - Checks and balances throughout a consensus standards development process serve as interim safeguards and ensure that the process can, in the end, withstand scrutiny. Internal and/or external review processes should be documented.
  - In addition to the opportunity for public comment, which NIST's processes clearly provide, the existence of a neutral oversight mechanism and/or an audit process would likely prove valuable.

- **Grievance/Appeals Process**
  - Whether and to what extent participants have recourse, such as the right to appeal, should be reflected in written procedures. A basic explanation of the option and how to access it should be presented.

- **Evidence of Compliance**
  - Documentation of compliance with established procedures allows a standards development process to be scrutinized objectively. Retention of evidence of procedural compliance for one complete standards cycle or until a standard is withdrawn is recommended.
  - An audit could enhance the integrity of the standards development process by objectively assessing evidence of compliance in relation to procedural and/or technical content issues.

Processes for Effectively Engaging Stakeholders

The competitions that NIST hosts are an excellent example of one way to engage stakeholders – domestically and internationally. Webinars are another important and readily accessible engagement mechanism, particularly when the goal is information dissemination. Social media is also recommended as a way to reach broad audiences at minimal cost.

Staff Training

Ongoing and regular training at all levels provides an essential safeguard for ensuring that procedures are understood and followed.

Assessment of NIST Cryptographic Materials, Noting When They Adhere to or Diverge from Those Principles and Processes

To the extent that some of the scenarios described by NIST acknowledge a degree of arbitrariness or lack of routine process, a more formal and detailed set of procedures combined with well-trained staff and public notice of applicable procedures would help guard against future claims of arbitrariness.

Conclusion

It is recognized that multiple paths to standardization exist. Many standards demand a voluntary consensus standards development process[2]; however, some standards, by nature, do not lend themselves to a transparent and due process–based consensus process. In some cases, collaborative relationships with formal standards development organizations – such as those referenced between NIST and ASC X9 Inc. or NIST and IEEE, respectively – may be most effective. NIST's unique role within the federal government and statutory responsibility with respect to cryptographic standards and guidelines certainly underscore the need for NIST to have the ability to choose to work in a range of standards development ecosystems, based on which process best suits its purposes.

In all cases, it seems that documentation of the criteria leading to the standards development process selection – including the key factors and actors that drive NIST's choice of development process combined with sufficiently documented procedures, adequate public notices, and consistent implementations – would help to avoid and dispel any future claim of a lack of transparency or arbitrariness.

Thank you again for the opportunity to participate on the COV.

[2] See the definition of voluntary consensus standards organization in OMB A-119, 1998 edition: http://www.whitehouse.gov/omb/circulars_a119