



COMPUTER SECURITY DIVISION

# ANNUAL REPORT 2015

THIS PAGE IS LEFT INTENTIONALLY BLANK.

COMPUTER SECURITY DIVISION

# ANNUAL REPORT 2015

**PATRICK O'REILLY, EDITOR**  
*Computer Security Division*  
*Information Technology Laboratory*

**CO-EDITORS:**  
Larry Feldman  
Greg Witte  
*G2, Inc.*  
*Annapolis Junction, Maryland*

THIS PUBLICATION IS AVAILABLE FREE OF CHARGE FROM  
<http://dx.doi.org/10.6028/NIST.SP.800-182>

JULY 2016



**U.S. DEPARTMENT OF COMMERCE**  
Penny S. Pritzker, Secretary

**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**  
Willie May, Under Secretary of Commerce for Standards and Technology and Director



## AUTHORITY

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-182  
Natl. Inst. Stand. Technol. Spec. Publ. 800-182, 120 pages (July 2016)  
CODEN: NSPUE2

This publication is available free of charge from:  
<http://dx.doi.org/10.6028/NIST.SP.800-182>

## REPORTS ON COMPUTER SYSTEMS TECHNOLOGY

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.





## ACKNOWLEDGMENTS

The editor, Patrick O'Reilly of the Computer Security Division, wishes to thank his colleagues in the Computer Security Division, who provided write-ups on their 2015 project highlights and accomplishments for this annual report (their names are mentioned after each project write-up). The editor would also like to acknowledge Elaine Barker (CSD), Lisa Carnahan (Standards Coordination Office, NIST), Greg Witte and Larry Feldman (G2) for reviewing and providing valuable feedback for this annual report.

The editor would also like to acknowledge Kristen Dill of Dill and Company, Inc. for designing the cover and inside layout for this 2015 annual report.

## DISCLAIMER

Any mention of commercial products or organizations is for informational purposes only; it is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the products identified are necessarily the best available for the purpose.

## TRADEMARK INFORMATION

All names are trademarks or registered trademarks of their respective owners.

# TABLE OF CONTENTS

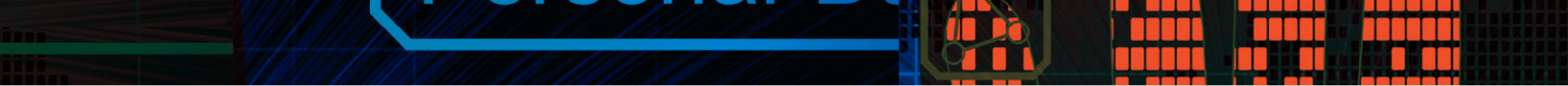
<b>DISCLAIMER .....</b>	<b>IV</b>
<b>ACKNOWLEDGMENTS .....</b>	<b>V</b>
<b>TRADEMARK INFORMATION .....</b>	<b>V</b>
<b>WELCOME LETTER .....</b>	<b>1</b>
<b>COMPUTER SECURITY DIVISION (CSD) ORGANIZATION .....</b>	<b>2</b>
<b>INTRODUCTION TO CSD'S FIVE GROUPS .....</b>	<b>3</b>
Cryptographic Technology Group (CTG) .....	4
Security Components and Mechanisms Group (SCMG) .....	4
Secure Systems and Applications Group (SSAG) .....	5
Security Outreach and Integration Group (SOIG) .....	6
Security Testing, Validation, and Measurement Group (STVMG) .....	7
<b>CSD IMPLEMENTS FEDERAL INFORMATION SECURITY MANAGEMENT ACT .....</b>	<b>8</b>
<b>PROGRAM AND PROJECT ACHIEVEMENTS FOR FY 2015 .....</b>	<b>11</b>
<b>NIST RESPONSIBILITIES UNDER EXECUTIVE ORDER 13636, "IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY" .....</b>	<b>12</b>
<b>CSD WORK IN NATIONAL AND INTERNATIONAL STANDARDS .....</b>	<b>13</b>
Identity Management Standards within INCITS B10 and ISO JTC1/SC17 .....	15
Cloud Computing Standards Developed by ISO/IEC JTC 1/SC 38 Cloud Computing and INCITS Cloud 38 .....	16
ISO Standardization of Security Requirements for Cryptographic Modules .....	16
<b>FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) IMPLEMENTATION PROJECT .....</b>	<b>18</b>
<b>BIOMETRIC STANDARDS AND ASSOCIATED CONFORMITY ASSESSMENT TESTING TOOLS .....</b>	<b>20</b>
<b>SECURITY OF CYBER-PHYSICAL SYSTEMS (CPS) .....</b>	<b>22</b>
<b>FEDERAL CYBERSECURITY RESEARCH &amp; DEVELOPMENT (R&amp;D) .....</b>	<b>23</b>
<b>SECURITY ASPECTS OF ELECTRONIC VOTING .....</b>	<b>23</b>
<b>HEALTH INFORMATION TECHNOLOGY SECURITY .....</b>	<b>24</b>
<b>SUPPLY CHAIN RISK MANAGEMENT (SCRM) FOR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) .....</b>	<b>25</b>
<b>NATIONWIDE PUBLIC SAFETY BROADBAND NETWORK (NPSBN) CYBERSECURITY .....</b>	<b>26</b>
<b>SMART GRID CYBERSECURITY .....</b>	<b>27</b>
<b>CYBERSECURITY AWARENESS, TRAINING, EDUCATION, AND OUTREACH .....</b>	<b>28</b>
National Initiative for Cybersecurity Education (NICE) .....	28
Computer Security Resource Center (CSRC) .....	29
Federal Computer Security Managers' (FCSM) Forum .....	29
Federal Information Systems Security Educators' Association (FISSEA) .....	30
Information Security and Privacy Advisory Board (ISPAB) .....	33
Small and Medium Size Business (SMB) Cybersecurity Outreach Workshop .....	35
<b>CRYPTOGRAPHIC STANDARDS PROGRAM .....</b>	<b>36</b>
Hash Algorithms and the Secure Hash Algorithm-3 (SHA-3) Standard (FIPS 202) .....	36
Random Number Generation (RNG) .....	36
Block Cipher Modes of Operation .....	37
Key Management .....	37
Transport Layer Security .....	38
Elliptic Curve Cryptography .....	38
Post-Quantum Cryptography .....	39
Circuit Complexity .....	40
Cryptography for Constrained Environments .....	41
The NIST Randomness Beacon .....	42
Entropy as a Service (EaaS) .....	43
Wireless and Mobile Security .....	44
Authentication .....	44



# TABLE OF CONTENTS

<b>VALIDATION PROGRAMS.....</b>	<b>46</b>
Cryptographic System Validation.....	46
Cryptographic Programs and Laboratory Accreditation.....	46
Automated Security Testing and Test Suite Development.....	51
Security Content Automation Protocol (SCAP) Validation Program.....	54
<b>IDENTITY MANAGEMENT .....</b>	<b>55</b>
NIST Personal Identity Verification Program (NPIVP).....	55
Personal Identity Verification (PIV) and FIPS 201 Revision Efforts.....	56
<b>RESEARCH IN EMERGING TECHNOLOGIES .....</b>	<b>57</b>
Secure Development Toolchain Competitions.....	57
Cloud Computing and Virtualization.....	58
CSD Role in the NIST Cloud Computing Program.....	58
Policy Machine – Leveraging Access Control for Cloud Computing.....	59
Security for a Virtualized Infrastructure.....	60
Cybersecurity for Emerging Technologies.....	60
Cyber Threat Information Sharing.....	61
The Ontology of Authentication.....	62
<b>MOBILE SECURITY .....</b>	<b>63</b>
<b>STRENGTHENING INTERNET SECURITY.....</b>	<b>63</b>
USGv6: A Technical Infrastructure to Assist IPv6 Adoption.....	63
<b>ACCESS CONTROL PROJECTS.....</b>	<b>64</b>
Access Control and Privilege Management.....	64
Conformance Verification for Access Control Policies.....	65
Attribute-Based Access Control.....	66
<b>ADVANCED SECURITY TESTING AND MEASUREMENTS .....</b>	<b>68</b>
Security Automation and Continuous Monitoring.....	68
Specification, Standards, and Guidance Development.....	68
Security Content Automation Protocol (SCAP).....	69
Software Asset Management Standards.....	71
Development of Security Automation Consensus Standards.....	71
Automation Reference Data.....	73
National Vulnerability Database (NVD).....	73
National Checklist Program (NCP).....	73
United States Government Configuration Baseline (USGCB) / FDCC Baselines.....	75
Apple OS X Security Configuration.....	75
<b>TECHNICAL SECURITY METRICS.....</b>	<b>76</b>
Security Risk Analysis of Enterprise Networks Using Attack Graphs.....	76
Algorithms for Intrusion Measurement.....	77
Automated Combinatorial Testing.....	78
Roots of Trust.....	78
<b>HONORS AND AWARDS.....</b>	<b>80</b>
<b>COMPUTER SECURITY DIVISION PUBLICATIONS .....</b>	<b>85</b>
FY 2015 Computer Security Division Publications.....	85
NIST Technical Series Publications – FIPS, SPs, NISTIRs, and ITL Bulletins.....	87
Federal Information Processing Standards (FIPS).....	91
NIST Special Publications.....	91
NISTIRs.....	97
Additional Publications by CSD Authors.....	99
Journal Articles.....	100
Conference Papers.....	102
Books and Book Sections.....	105
White Papers.....	105
<b>ACRONYMS.....</b>	<b>106</b>
<b>OPPORTUNITIES TO ENGAGE WITH CSD, ACD, AND NIST DURING FY 2016.....</b>	<b>111</b>





THIS PAGE IS LEFT INTENTIONALLY BLANK.

## WELCOME LETTER

The Computer Security Division (CSD), a division of the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) is responsible for developing cybersecurity standards, guidelines, tests, and metrics for the protection of non-national security federal information systems. CSD's standards, guidelines, tools and references are developed in an open, transparent, traceable and collaborative manner that enlists broad expertise from around the world. While developed for federal agency use, these resources are voluntarily adopted by other organizations because they are effective and accepted globally.

The need for cybersecurity standards, best practices, tools and references that also address interoperability, usability and privacy continue to be critical for the Nation. CSD aligns its resources to enable greater development and application of practical, innovative security technologies and methodologies that enhance our ability to address current and future computer and information security challenges. Our foundational research and applied cybersecurity programs continue to advance in many areas, including cryptography, automation, roots of trust, identity and access management, advanced security testing and measurement, Internet of Things (IoT), cyber-physical systems, and public safety networks.

Trust is crucial to the broad adoption of our standards and guidelines, including our cryptographic standards and guidelines. To ensure that our cryptography resources have been developed according the highest standard of inclusiveness, transparency and security, NIST conducted an internal and external formal review of our cryptographic standards development efforts in 2014. We documented and solicited public comment on the principles and rigorous processes we use to engage stakeholders and experts in industry, academia, and government to develop and revise these standards. The final report is now published and serves as a basis for all CSD's cryptographic development efforts.

Increasing the trustworthiness and resilience of the IT infrastructure is a significant undertaking that requires a substantial investment in the architectural design and development of our systems and networks. A disciplined and structured set of systems security engineering processes that starts with and builds on well-established international standards provides an important starting point. Draft Special Publication 800-160, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*, which was issued in May 2014, helps organizations to develop a more defensible and survivable information technology infrastructure. This resource, coupled with other NIST standards and guidelines, contributes to systems that are more resilient in the face of cyber attacks and other threats.

Strong partnerships with diverse stakeholders are vital to the success of our technical programs. In February 2014, NIST issued the Framework for Improving Critical Infrastructure Cybersecurity as directed in Executive Order 13636. The Framework, created through collaboration between industry and government, consists of standards, guidelines, and practices to promote the protection of the critical infrastructure. Its approach helps owners and operators of the critical infrastructure to manage cybersecurity-related risk.

Active engagement with diverse stakeholders continues to be critical to our success. In the federal space, this interaction is most prominent in our strengthened collaborations with the Department of Defense, the Intelligence Community, and the Committee on National Security Systems to establish a common foundation for information security across the Federal Government. Our cybersecurity awareness, training, and education programs also exemplify the importance of engagements with academic institutions, federal agencies, small and medium businesses and others to increase awareness and enhance the overall cybersecurity posture of the Nation. CSD's work with Health and Human Services, Department of Transportation, Federal Communications Commission and others are all examples of an active and strong engagement, applying security to multiple government mission areas.

For many years, CSD, in collaboration with our global partners across industry, academia, standards bodies, and government, has made great contributions to help secure the nation's critical information and infrastructure. We look forward to strengthening these relationships as we lead the development and practical application of scalable and sustainable information security standards and practices.



**Matthew Scholl**  
Division Chief

# COMPUTER SECURITY DIVISION (CSD) ORGANIZATION



## MATTHEW SCHOLL

Chief, Computer Security Division  
Deputy Chief, Computer Security Division and  
Acting Associate Director of Operations,  
National Cybersecurity Center of Excellence

## GROUP MANAGERS



## LILY CHEN

(Acting Group Manager)  
Cryptographic Technology Group



## DAVID FERRAILOLO

Secure Systems and  
Applications Group



## MARK (LEE) BADGER

Security Components and  
Mechanisms Group



## KEVIN STINE<sup>1</sup>

Security Outreach and  
Integration Group<sup>2</sup>



## MICHAEL COOPER

Security Testing, Validation  
and Measurement Group

\*\* Editor's Note:

1: In FY 2016 (starting October 1, 2015), Kevin Stine has been selected to be the division chief for the new division in the Information Technology Laboratory (ITL). This new division is the Applied Cybersecurity Division.

2: During FY 2016, Mr. Jon Boyens will be the Acting Group Manager until a new group manager has been selected.





## INTRODUCTION TO CSD'S FIVE GROUPS

The Computer Security Division's computer scientists, mathematicians, IT specialists, support staff and others support CSD's mission and responsibilities through five groups that are described in the following sections:

- Cryptographic Technology Group
- Security Components and Mechanisms Group
- Secure Systems and Applications Group
- Security Outreach and Integration Group
- Security Testing, Validation, and Measurement Group

## CRYPTOGRAPHIC TECHNOLOGY GROUP (CTG)

### MISSION STATEMENT:

**Research, develop, engineer, and standardize cryptographic algorithms, methods, and protocols.**

### OVERVIEW:

The Cryptographic Technology Group's (CTG) work in the field of cryptography includes researching, analyzing and standardizing cryptographic technology, such as hash algorithms, symmetric and asymmetric cryptographic techniques, key management, authentication, and random number generation. The CTG's goal is to identify and promote methods to protect communications and storage through cryptographic technologies, encouraging innovative development and helping technology users to manage risk.

In FY 2015, the CTG continued to collaborate with national and international government agencies, academic and research organizations, industry partners, and standards bodies to develop interoperable security standards and guidelines, and to make an impact in the field of cryptography. One example is the culmination of an eight-year standardization effort that led to the publication of Federal Information Processing Standard (FIPS) 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, announced in the Federal Register on August 5, 2015.

The CTG's cryptographic standards program focuses on cryptographic primitives, algorithms, and schemes; the developed standards and guidelines are specified in FIPSs, NIST Special Publications (SPs), and NIST Interagency or Internal Reports (NISTIRs). Such standards and guidelines have been considered or adopted by the information technology (IT) industry and standards development organizations, such as the International Organization for Standardization (ISO), the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), and the Trusted Computing Group (TCG), and have been implemented on a variety of platforms.

The CTG is committed to the development of its standards using an open and transparent process - conducting workshops and requesting input and comments from government agencies, private industry, academia and the global cryptographic community. The CTG also examines each of its standards to determine if they need to be revised, withdrawn or re-opened for public comment.

The CTG continues to develop expertise in several critical research areas, such as post-quantum cryptography

(PQC), elliptic curve cryptography (ECC), privacy-enhancing cryptography, and lightweight cryptographic schemes for constrained environments. It has collaborated with many universities internationally and presented research results in major cryptography conferences and journals. In addition, it organized workshops on PQC, ECC standards, and lightweight cryptography to discuss research results and develop standardization roadmaps.

The CTG also published several guidelines on cryptographic applications, including key management, public key certificate policies, and trusted platforms. The CTG also participated in the cybersecurity projects of other CSD groups, such as the Personal Identity Verification (PIV) standards, the Federal Cloud Credential Exchange (FCCX), the Cryptographic Algorithm Validation Program (CAVP), and the Cryptographic Module Validation Program (CMVP).

### GROUP MANAGER (ACTING):

Dr. Lily Chen  
(301) 975-6974  
lily.chen@nist.gov

## SECURITY COMPONENTS AND MECHANISMS GROUP (SCMG)

### MISSION STATEMENT:

**Research, develop, and standardize foundational security mechanisms, protocols, and services.**

### OVERVIEW:

The SCMG's security research focuses on the development and management of foundational building-block security mechanisms and techniques that can be integrated into a wide variety of mission-critical U.S. information systems. The group's work spans the spectrum from near-term hardening and improvement of systems, to the design and analysis of next-generation, leap-ahead security capabilities. Computer security depends fundamentally on the level of trust of computer software and systems. This work, therefore, focuses strongly on assurance-building activities ranging from the analysis of software configuration settings, to advanced trust architectures, and to testing tools that identify flaws in software modules. This work also focuses significantly on increasing the applicability and effectiveness of automated techniques, wherever feasible. The SCMG conducts collaborative research with government, industry, and academia. Outputs of this research consist of prototype systems, software tools, demonstrations, guidelines, and other documentary resources.

Collaborating extensively with government, academia, and the private sector, SCMG works on a variety of topics, such as:

- Specifications for the automated exchange of security information between systems;
- Threat information sharing guidelines;
- Formulation of high-assurance software configuration settings;
- Hardware roots-of-trust for mobile devices;
- Secure Basic Input Output System (BIOS) layers;
- Combinatorial testing techniques;
- Conformity assessment of software implementing biometric standards; and
- Adoption of Internet Protocol Version 6 and Internet Protocol security extensions.

In FY 2015, collaborators and the associated collaborations have included Carnegie Mellon University (test development environment), Johns Hopkins Applied Physics Lab (the practical application of a combinatorial coverage measurement tool), the University of Texas at Arlington (a covering array generation algorithm), Mexico's Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional (a very large covering array generation and its application to hardware malware detection), Lockheed Martin Corporation (the practical application of covering arrays), United States Marine Corps (USMC) Camp Pendleton (testing and fault location for the tactical data link TADIL-J protocol), University of Texas Dallas and East Carolina University (safety-critical systems testing), Duke University (analysis of software failures), the National Science Foundation (cybersecurity metrics and assurance building), the National Security Agency (NSA) Information Assurance Directorate (security automation standardization), the Department of Homeland Security (DHS) Cybersecurity and Communications (security automation standardization), and DHS (incident coordination).

SCMG accomplishments include results of a 2.5-year study with Lockheed Martin (CRADA) showing 20 % test cost reduction with 20 % to 50 % improvement in coverage (8 pilot projects), an analysis of Internet resilience to connectivity disruption attacks, and release of software to test conformance to the newest version of the ANSI/NIST-ITL 1 Biometric Standard.

## GROUP MANAGER:

Mr. Mark (Lee) Badger  
(301) 975-3176  
lee.badger@nist.gov

## SECURE SYSTEMS AND APPLICATIONS GROUP (SSAG)

### MISSION STATEMENT:

**Integrate and apply security technologies, standards and guidelines for computing platforms and information systems.**

### OVERVIEW:

SSAG's security research focuses on identifying emerging and high-priority technologies, and on developing security solutions that will have a high impact on U.S. critical infrastructure. The group conducted research and development related to both public and private sector use cases. The research considered many aspects of the system's lifecycle from the earliest stages of technology development through proof-of-concept, reference and prototype implementations, and demonstrations. In addition, the group worked to transfer new technologies to industry; to produce new standards and guidance for federal agencies and industry; and to develop tests, test methodologies, and assurance methods.

SSAG investigated security concerns associated with such areas as mobile devices, cloud computing and virtualization, identity management, access control and authorization management, and software assurance. SSAG's research helps to meet federal information security requirements that may not be fully addressed by existing technology. The group collaborated extensively with government, academia, and private sector entities.

Example successes from this work include:

- Tools for access control policy testing;
- New concepts in access control and policy enforcement;
- Several Personal Identity Verification (PIV) documents to support interagency use of the PIV Card;
- Methods for architecting a secure cloud ecosystem in a capability-oriented approach;
- Guidance and tools for orchestrating a secure cloud ecosystem;
- Guidance for secure deployment of virtualized infrastructure components – Hypervisor, Virtual Machines (VMs) and Virtual Network;
- Methods for achieving comprehensive policy enforcement and data interoperability across enterprise data services; and



- Test methods for mobile device (smart phone) application security.

In particular, the SSAG led the NIST Security and Forensics Working Group that published draft NISTIR 8006, *NIST Cloud Computing - Security Reference Architecture*, that aggregates forensics challenges in a cloud ecosystem. The working group has been working on developing a draft of SP 800-173, *Guidance for Applying the Risk Management Framework to Federal-based Information Systems* (target release date: spring/summer 2016). In response to the rapidly emerging use of virtualization in enterprise data centers for supporting both in-house mission-critical applications and for providing cloud services, two guidance documents were published: Draft SP 800-125A, *Security Recommendations for Hypervisor Deployment*, and Draft SP 800-125B, *Secure Virtual Network Configuration for Virtual Machine (VM) Protection*. In support of the revised FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, two new PIV-related SP 800-series were released and five SP 800 documents were revised. One of the new publications, SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, guides the implementation and deployment of PIV credentials for mobile devices. In addition, the PIV team participated in the Office of Management and Budget (OMB) cybersecurity Sprint effort with a goal to strengthen the cybersecurity of federal networks, systems, and data through multi-factor authentication using the PIV Card. To improve access to new technologies, the group also chaired, edited, and participated in the development of a wide variety of national and international security standards.

## GROUP MANAGER:

Mr. David Ferraiolo  
(301) 975-3046  
david.ferraiolo@nist.gov

## SECURITY OUTREACH AND INTEGRATION GROUP (SOIG)

### MISSION STATEMENT:

**Develop, integrate, and promote the mission-specific application of information security standards, guidelines, best practices, and technologies.**

### OVERVIEW:

The U.S. economy, citizens, and government rely on information technology (IT), so the protection of IT and the information infrastructure is critical. SOIG leverages broad cybersecurity and risk management expertise to develop, integrate, and promote security standards, guidelines, tools, technologies, methodologies, tests, and measurements to address cybersecurity needs in many areas of national and international importance.

The SOIG collaborates with stakeholders to address cybersecurity considerations in many diverse program areas, including the Information and Communications Technologies (ICT) supply chain, Smart Grid, Electronic Voting, Cyber Physical and Industrial Control Systems, Health Information Technology, and the National Public Safety Broadband Network. The group produces standards and guidelines through the Federal Information Security Management Act (FISMA) implementation program to help federal agencies build strong cybersecurity risk management programs. In each of these program areas, the group extends outreach to stakeholders across federal, state, and local governments; industry; academia; small businesses; and the public. The SOIG also leads several broad cybersecurity awareness, training, education, and outreach efforts, including the National Initiative for Cybersecurity Education (NICE), the Federal Computer Security Managers' Forum, and the Federal Information Systems Security Educators' Association (FISSEA).

Key to the group's success is the ability to interact with a broad constituency to ensure that SOIG's program is consistent with national objectives related to or impacted by information security. Through open and transparent public engagement, collaboration, and cooperation, the group works to address critical cybersecurity challenges, enable greater U.S. industrial competitiveness, and facilitate the practical implementation of scalable and sustainable information security standards and practices.

## GROUP MANAGER:

Mr. Kevin Stine  
(301) 975-4483  
kevin.stine@nist.gov

# SECURITY TESTING, VALIDATION, AND MEASUREMENT GROUP (STVMG)

## MISSION STATEMENT:

Advance information security testing, measurement science, and conformance.

## OVERVIEW:

Federal agencies, industry, and the public rely on cryptography for the protection of the information and communications used in electronic commerce, the critical infrastructure, and other application areas. The STVMG supports the testing and validation of the underlying cryptographic modules and cryptographic algorithms based upon established standards. These cryptographic modules and algorithms enable products and systems to provide security services, such as confidentiality, integrity protection, and authentication. Although cryptography provides security, poor designs or weak algorithms can render a product insecure and place highly sensitive information at risk. When protecting sensitive data, federal agencies require assurance that cryptographic products meet established security requirements and use only tested and validated cryptographic modules.

STVMG's testing-focused activities include validating cryptographic algorithm implementations, cryptographic modules, and Security Content Automation Protocol (SCAP)-enabled products; developing test suites and test methods; providing implementation guidance and technical support to industry forums; and conducting education, training, and outreach programs.

STVMG's validation programs work together with independent cryptographic and security testing laboratories accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP). Based on the independent laboratory test report and test evidence, the Validation Program validates an implementation under test. NIST publishes lists of awarded validations through public websites.

---

## GROUP MANAGER:

Mr. Michael Cooper  
(301) 975-8077  
michael.cooper@nist.gov



# Personal Data

THE COMPUTER SECURITY DIVISION  
IMPLEMENTS THE FEDERAL INFORMATION  
SECURITY MANAGEMENT ACT



## CSD IMPLEMENTS THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT

The E-Government Act, Public Law 107-347, passed by the 107th Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) of 2002, included the duties and responsibilities for the National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division (CSD). In December 2014, the 113th Congress updated FISMA as the Federal Information Security Modernization Act (Public Law 113-283). NIST CSD responsibilities were unchanged in the update. In 2015, CSD addressed its assignments through the following activities:

- One final Federal Information Processing Standard (FIPS) was issued: FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, which specifies the Secure Hash Algorithm-3 (SHA-3) family of functions on binary data. Each of the SHA-3 functions is based on an instance of the **KECCAK** algorithm that NIST selected as the winner of the SHA-3 Cryptographic Hash Algorithm Competition. (Note: FIPS 186-4, *Digital Signature Standard (DSS)*, which was published in 2013, was updated in 2015 to require the implementation of either FIPS 186 or FIPS 202 wherever a secure hash algorithm is required for Federal applications.)
- Thirty draft and final NIST Special Publications (SP) were issued that provide management, operational, and technical security guidelines in areas such as trustworthy email, media sanitization, protecting controlled unclassified information, supply chain risk management, assessing security and privacy controls, cryptographic algorithms and key lengths, key management systems, cyber threat information sharing, virtual machine protection, secure hypervisor deployment, random number generation, personal identity verification (PIV) (interfaces, credentials, card application and middleware), industrial control systems, the national checklist program, vetting the security of mobile applications, a biometric conformance testing methodology framework, attribute-based access control, access management for electric utilities, and securing electronic health records on mobile devices.
- Eighteen draft and final NIST Interagency/Internal Reports (NISTIR) were issued on a variety of topics,

including the National Strategy for Trusted Identities in Cyberspace (NSTIC) pilots for catalyzing the identity ecosystem, the proceedings of a symposium for cybersecurity for direct digital manufacturing, a summary of the executive technical workshop on improving cybersecurity and consumer privacy and the next steps in the process, risk management for replication devices, considerations for identity management in public-safety mobile networks, a summary of a public-safety mobile-application security requirements workshop, privacy risk management, cardholder authentication for the PIV digital signature key, derived PIV credentials proof-of-concept research, an advanced metering infrastructure smart meter upgradeability test framework, a report on strategic U.S. Government engagement in international standardization to achieve U.S. objectives for cybersecurity, guidelines for the creation of interoperable software identification (SWID) tags, a security content automation protocol (SCAP) Version 1.2 content style guide about best practices for creating and maintaining SCAP 1.2 content, de-identification of personally identifiable information, the security of interactive and automated access management using secure shell (SSH), a proof-of-concept implementation of trusted geolocation in the cloud, and fundamentals of small business information security.

- Continued the successful collaboration with the Department of Defense (DOD), the Intelligence Community (IC), and the Committee on National Security Systems (CNSS), in partnership with the Joint Task Force (JTF) Transformation Initiative. Five Special Publications are currently recognized as JTF publications, and the JTF partners continue to develop and update key cybersecurity guidelines for protecting federal information and information systems as part of the Unified Information Security Framework through CSD's FISMA Implementation Project.
- Continued to develop expertise in several critical research areas, such as post-quantum cryptography (PQC), elliptic curve cryptography (ECC), privacy-enhancing cryptography, and lightweight cryptographic schemes for constrained environments.
- Performed research and conducted outreach on standards, practices, and technologies to enable prompt and effective threat information sharing, hardware roots of trust for mobile devices, Internet of things, combinatorial testing techniques, cloud computing and virtualization, risk management, identity management, access control and authorization management, and software assurance.

- Supported the joint National Telecommunications and Information Administration (NTIA) and NIST Public Safety Communications Research (PSCR) program with efforts in public-safety mobile-application security, identity management, and enabling cybersecurity capabilities on the PSCR 700 MHz LTE network.
- Provided awareness support for the Cybersecurity Framework and encouraged its use as a tool to help industry sectors and organizations manage cybersecurity risks.
- Conducted workshops, awareness briefings, and outreach to CSD customers to ensure the comprehension of standards and guidelines, to share ongoing and planned activities, and to aid in scoping guidelines in a collaborative, open, and transparent manner. CSD public workshops addressed a diverse range of information security and technology topics, including cloud and mobile technologies; the cybersecurity framework; chain risk management; cybersecurity innovations; computer security awareness, training, and education forums and various events; safeguarding health information; Special Publications to support FIPS 201-2; post-quantum computing; direct digital manufacturing; elliptic curve cryptography standards; and lightweight cryptography to discuss research results and develop standardization roadmaps.
- Engaged with international standards bodies in a variety of areas, including promoting a broader international adoption of security automation specifications. Additionally, NIST's CSD continued to lead the Cryptographic Module Validation Program (CMVP), in conjunction with the Government of Canada's Communications Security Establishment. The Common Criteria Evaluation and Validation Scheme (CCEVS) and CMVP facilitate the security testing of IT products usable by the Federal Government.
- Provided assistance to agencies and the private sector through many outreach programs, including the National Initiative for Cybersecurity Education (NICE), the Federal Information Systems Security Educators' Association (FISSEA), and the Federal Computer Security Managers' Forum.
- Solicited recommendations from the Information Security and Privacy Advisory Board (ISPAB) on draft standards and guidelines, and on information security and privacy issues.
- The CSD 2015 annual report was produced and released as a NIST SP. CSD annual reports from fiscal years 2003 through 2015 are available on the Computer Security Resource Center (CSRC) at <http://csrc.nist.gov/publications/PubsTC.html#Annual Reports>.



# PROGRAM AND PROJECT ACHIEVEMENTS FOR FISCAL YEAR 2015



## PROGRAM AND PROJECT ACHIEVEMENTS FOR FY 2015

In FY 2015, CSD continued to research and develop guidance for a broad array of technical areas, including supply chain risk management; security analytics; cloud, mobile, and privacy-enhancing technologies; hardware-enabled security; and cyber-physical and embedded systems. CSD staff and guest researchers have collaborated with global partners from government, industry, and academia, making significant contributions to help secure critical information and the infrastructure. The following sections describe CSD's programs and project achievements, including extensive research and development for high quality, cost-effective security and privacy mechanisms, standards, guidelines, tests, and metrics that address current and future computer and information security challenges.

## NIST RESPONSIBILITIES UNDER EXECUTIVE ORDER 13636, "IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY"

Recognizing that the national and economic security of the United States depends on the reliable functioning of its critical infrastructure, the President issued Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, in February 2013. This EO directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices – for reducing cybersecurity risks to the critical infrastructure.

The Cybersecurity Framework (CSF) that was developed provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to help critical infrastructure owners, operators and other interested entities identify, assess, and manage cybersecurity-related risk, while protecting business confidentiality, individual privacy, and civil liberties.

In FY 2015, NIST continued to work with a diverse stakeholder community to support CSF use and understanding. This process included:

- Hosting a workshop at the University of South Florida in Tampa to share initial CSF experiences;
- Updating the CSF Web site with a catalog of industry resources, upcoming NIST speaking events, and an extensive frequently-asked-question knowledge base;

- Coordinating with critical infrastructure owners and operators, regulators, and other industry organizations through a variety of meetings and industry events to ensure understanding and use;
- Analyzing various industry work products, such as mapping documents, for CSF correctness;
- Consulting with state and local governments, and the governments of other nations regarding their alignment with both the principles and the cybersecurity outcomes of the CSF;
- Consulting with international organizations and standards bodies to demonstrate and ensure continued alignment with voluntary international standards; and
- Working with both industry and regulatory organizations to apply the CSF in ways that bring efficiencies to the regulatory process.

Since the release of the Framework, NIST's primary goal has been to raise awareness of the Framework and encourage its use as a tool to help industry sectors and organizations manage cybersecurity risks. NIST has strengthened its collaboration with critical infrastructure owners and operators, industry leaders, government partners, and other stakeholders, building on previous years' interactions that were crucial to the Framework's development.

In FY 2016, NIST will continue to conduct stakeholder outreach and will work collaboratively to further understand stakeholder needs regarding tools and resources to enable more effective use of the Framework. NIST will also publish guidance on how NIST's Risk Management Framework (SP 800-37 revision 1) and the Cybersecurity Framework complement each other. Additionally, NIST will formally gather stakeholder input about Framework use, evolution, and future management through a request for information (RFI). Following the RFI, NIST will conduct a public workshop at NIST in Gaithersburg, Maryland on April 6 and 7, 2016. Periodic program updates will be provided through the Framework website.

### For More Information, See:

<http://www.nist.gov/cyberframework>

## CONTACTS:

Mr. Matt Barrett  
301) 975-6259  
[matthew.barrett@nist.gov](mailto:matthew.barrett@nist.gov)

Mr. Adam Sedgewick  
(301) 367-4678  
[adam.sedgewick@nist.gov](mailto:adam.sedgewick@nist.gov)



# CSD WORK IN NATIONAL AND INTERNATIONAL STANDARDS

## CSD's Part in National and International ISO Security Standards Processes

Figure 1 shows many of the national and international standards developing organizations (SDOs) involved in cybersecurity standardization. CSD participates in many cybersecurity standards' activities in many of these organizations, either in leadership positions or as editors and contributors, including the Biometric Application Programming Interface (BioAPI) Consortium; the Bluetooth Special Interest Group (SIG); Bluetooth Security Expert Group (BT-SEG); the International Telecommunications Union - Telecommunication Standardization Sector (ITU-T); various groups within the Institute of Electrical and Electronics Engineers (IEEE) and the Internet Engineering Task Force (IETF); the North American Security Products Organization (NASPO); the Trusted Computing Group (TCG);

and Accredited Standards Committee X9, Inc. (ASC X9, Inc.) (e.g., X9F – Data & Information Security Subcommittee). Many of CSD's publications have been the basis for both national and international standards projects.

The following paragraphs discuss, in particular, CSD staff activities in conjunction with the InterNational Committee for Information Technology Standards (INCITS) Technical Committee Cyber Security (CS1), where CSD's Sal Francomacaro served as the CS1 Vice Chair.

## The International Organization for Standardization (ISO)

The International Organization for Standardization (ISO) is a network of the national standards institutes of 148 countries, with representation by one member per country. The scope of ISO covers the standardization in all fields except electrical and electronic engineering standards, which are the responsibility of the International Electrotechnical Commission (IEC).

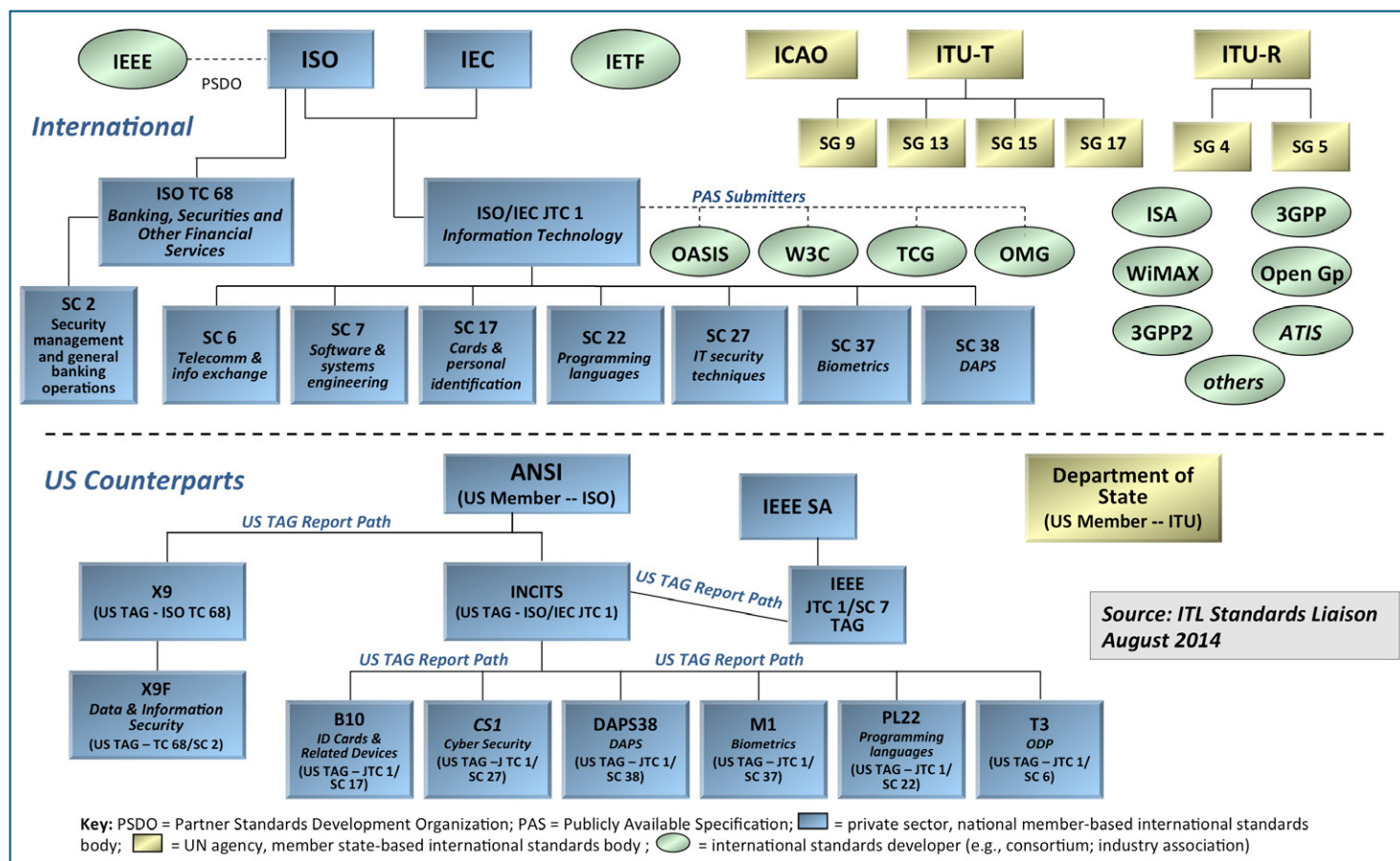


Figure 1: SDOs involved in Cybersecurity

The IEC prepares and publishes international standards for all electrical, electronic, and related technologies, including electronics, magnetics and electromagnetics, electroacoustics, multimedia, telecommunication, and energy production and distribution, as well as associated general disciplines, such as terminology and symbols, electromagnetic compatibility, measurement and performance, dependability, design and development, safety, and the environment. (see <http://www.iec.ch/about/>).

Joint Technical Committee 1 (JTC 1) was formed by ISO and IEC to be responsible for international standardization in the field of Information Technology (see [http://www.iso.org/iso/jtc1\\_home.html](http://www.iso.org/iso/jtc1_home.html)). JTC 1 develops, maintains, promotes, and facilitates the IT standards required by global markets, meeting business and user requirements concerning:

- Design and development of IT systems and tools;
- Performance and quality of IT products and systems;
- Security of IT systems and information;
- Portability of application programs;
- Interoperability of IT products and systems;
- Unified tools and environments;
- Harmonized IT vocabulary; and
- User-friendly and ergonomically designed user interfaces.

JTC 1 consists of a number of subcommittees (SCs) and working groups that address specific technologies. SCs that produce standards relating to IT security include:

- SC 06 - Telecommunications and Information Exchange Between Systems;
- SC 17 - Cards and Personal Identification;
- SC 27 - IT Security Techniques; and
- SC 37 - Biometrics (Note: Fernando Podio, NIST CSD, served as Chair).

JTC 1 also has:

- Technical Committee 68 - Financial Services;
- SC 2 - Operations and Procedures, including Security;
- SC 4 - Securities;
- SC 6 - Financial Transaction Cards, Related Media and Operations;
- SC 7 - Software and Systems Engineering; and
- SC 38 - Distributed application platforms and services (DAPS).

## The American National Standards Institute (ANSI)

The American National Standards Institute (ANSI) is a private, nonprofit (501(c)(3)) organization that administers and coordinates the U.S. voluntary standardization and conformity assessment system, and facilitates the development of American National Standards (ANSs) by accrediting the procedures of SDOs.

ANSI promotes the use of U.S. standards internationally, advocates U.S. policy and technical positions in international and regional standards organizations, and encourages the adoption of international standards as national standards where they meet the needs of the U.S. user community. ANSI is the sole U.S. representative and dues-paying member of the two major non-treaty international standards organizations: ISO and, via the United States National Committee (USNC), the IEC.

INCITS is an ANSI-accredited SDO that serves as the ANSI Technical Advisory Group (TAG) for ISO/IEC Joint Technical Committee 1. INCITS is sponsored by the Information Technology Industry (ITI) Council, a trade association representing the leading U.S. providers of information technology products and services.

INCITS is organized into Technical Committees that focus on the creation of standards for different technology areas. Technical committees that focus on IT security and IT security-related technologies, or that may require separate security standards include:

- B10 - Identification Cards and Related Devices;
- CS1 - Cyber Security (Dan Benigni, NIST CSD, Chair; Sal Francomacaro, NIST CSD, Vice Chair and NIST Principal Voting Member);
- E22 - Item Authentication;
- M1 - Biometrics (Fernando Podio, NIST CSD, Chair);
- T3 - Open Distributed Processing (ODP);
- T6 - Radio Frequency Identification (RFID) Technology;
- GIT1 - Governance of IT; and
- DAPS38 - Distributed Application Platforms and Services.

As a technical committee of INCITS, CS1 develops national, ANSI-accredited standards in the area of cybersecurity. Its scope encompasses:

- Management of information security and systems;
- Management of third-party information security service providers;
- Intrusion detection;

- Network security;
- Cloud computing security;
- Supply-chain risk management;
- Incident handling;
- IT security evaluation and assurance;
- Security assessment of operational systems;
- Security requirements for cryptographic modules;
- Protection profiles;
- Role-based access control;
- Security checklists;
- Security metrics;
- Cryptographic and non-cryptographic techniques and mechanisms, including confidentiality, entity authentication, non-repudiation, key management, data integrity, message authentication, hash functions, and digital signatures;
- Future service and application standards supporting the implementation of control objectives and controls, as defined in ISO 27001, in the areas of business continuity and outsourcing;
- Identity management, including an identity management framework, role-based access control, and single sign-on; and
- Privacy technologies, including a privacy framework, privacy reference architecture, privacy infrastructure, anonymity and credentials, and specific privacy-enhancing technologies.

Several members of NIST's CSD staff contribute to CS1's national and international IT security standards efforts through its membership in CS1.

## CSD's Role in Cybersecurity Standardization

CSD's cybersecurity research also plays a direct role in the Cybersecurity Standardization efforts of CS1 at the national level. The following is a description of the national-level progress achieved during FY 2015 by CSD and CS1.

The NIST Policy Machine research and development effort has resulted in three ongoing national standards projects in CS1 in the early stages of development. They include:

- *Next Generation Access Control -Functional Architecture (NGAC-FA)*, project number INCITS 499-2013, was published in FY 2013 and is recently beginning an early revision.

- *Next Generation Access Control - Generic Operations & Abstract Data Structures (NGAC-GOADS)*. Serban Gavrila, NIST CSD, is the editor. The project is assigned project number 2195-D, and the document (planned for publication in FY 2016) has successfully completed two public review periods.
- *Next Generation Access Control -Implementation Requirements, Protocols and API Definitions (NGAC-IR-PADS)*. Project number is 2193-D has been assigned.

Sal Francomacaro also served as cybersecurity standards coordinator in CSD.

## CONTACT:

Mr. Salvatore Francomacaro  
(301) 975-6414  
salvatore.francomacaro@nist.gov

## Identity Management Standards within INCITS B10 and ISO JTC1/SC17

CSD supports identity management standardization activities through participation in national and international standards bodies and organizations. CSD actively participates in the INCITS B10 committee, which is focused on the interoperability of Identification Cards and Related Devices. CSD has contributed and provided valuable feedback to many INCITS B10 standards during the development process. In addition, CSD also actively participates in the B10.8 and B10.12 committees.

The INCITS/B10.8 committee works on International Driver's License standards and serves as the U.S. Technical Advisory Group (TAG) to the ISO/IEC JTC 1/SC 17 Working Group (WG) 10 efforts on the International Standardization of Driver's License documents. The B10.12 committee develops interoperable standards for Integrated Circuit Cards with Contacts, and serves as the U.S. TAG for the international ISO/IEC JTC 1 SC 17 Working Groups 4 and 11. During FY 2015, Mr. Francomacaro served as the U.S. Head of delegation to ISO/IEC JTC 1 SC 17 WG4 and WG11.

CSD provides technical and editorial support in the development of national and international standards. Specifically, Mr. Ketan Mehta, a CSD staff member, serves as the technical editor of ANSI 504-1, *Generic Identity Command Set (GICS)*. GICS enables PIV, PIV-Interoperable (PIV-I) and Common Access Card (CAC) applications, and others, to be built from a single platform. GICS defines an open platform where identity applications can be instantiated, deployed, and used in an interoperable way between the credential issuers and credential users. During FY 2015, an amendment process was started on INCITS 504



Parts 1 and 2 to better align them with the new NIST SP 800-73-4 (PIV) specifications.

CSD staff also provided significant input to the standards of major interest to U.S. government agencies and U.S. markets. CSD played a role in the development and revision of:

- ISO/IEC 7816 (Identification Cards, Integrated Circuit Cards);
- ISO/IEC 18013 (Personal Identification, ISO Compliant Driving License);
- ISO/IEC 19286 (Identification cards, Privacy-enhancing protocols and services);
- Doc 9303-10 LDS 2 (Machine Readable Travel Documents Logical Data Structure for Storage of Data in Contactless Interface);
- ISO/IEC 24727 (Identification Cards, Integrated Circuit Card Programming Interfaces); and
- ISO/IEC 24787 (Biometrics “Match On Card” Comparison).

During FY 2016, the INCITS B10 committee, along with the active collaboration of CSD staff, plans to:

- Publish Part 3 of INCITS 504;
- Complete the amendment process for INCITS 504 Part 1 and 2;
- Contribute to the publication of several revisions of the ISO/IEC 7816 family of standards (all relevant to FIPS 201 specifications);
- Pursue the standardization and harmonization of identity standards developed in the U.S.;
- Develop requirements and identify standards gaps for Mobile Driving Licenses;
- Enhance the Machine Readable Travel Documents (ePassport) data model to address privacy and security concerns; and
- Contribute to the development of privacy-enhanced security protocols.

CSD staff will continue to actively support relevant ID management standard initiatives, such as ISO/IEC 19286 (Integrated Circuit Card (ICC) Privacy-enhancing protocols and services) and ISO/IEC 18328 (ICC managed Devices).

CSD’s investment in these activities is motivated by new technical ideas that emerge from these ISO standards. For example, INCITS 504 is an ID platform that leverages the FIPS 201 infrastructure to support a large number of government

and enterprise initiatives. In particular, INCITS 504 aims to support initiatives such as the National Strategy for Trusted Identities in Cyberspace (NSTIC). ISO/IEC 24727 aims to create an interoperability framework that increases the resilience and scalability of identity management solutions and to foster domestic and international interoperability.

---

## CONTACTS:

Mr. Salvatore Francomacaro (301) 975-6414 salvatore.francomacaro@nist.gov	Mr. Ketan Mehta (301) 975-8405 ketan.mehta@nist.gov
---	---

## Cloud Computing Standards Developed by ISO/IEC JTC 1/SC 38 Cloud Computing and INCITS Cloud 38

NIST has been designated by the Federal Chief Information Officer (CIO) to accelerate the Federal Government’s secure adoption of cloud computing by leading efforts to identify existing standards and guidelines. Where international standards are needed, NIST works closely with U.S. industry, standards developers, other government agencies, and leaders in the global standards community to develop standards that will support secure cloud computing.

As part of this program, Ms. Annie Sokol, CSD, provides technical and editorial representation in the development of national and international standards in both SC 27 and SC38. She was the convener for ISO/IEC 17788 Information technology – *Cloud Computing Overview and vocabulary*, which is the normative reference to other published and under-development.

---

## CONTACT:

Ms. Annie Sokol  
(301) 975-2006  
annie.sokol@nist.gov

## ISO Standardization of Security Requirements for Cryptographic Modules

CSD has contributed to the activities of ISO/IEC JTC 1 SC/27, which published ISO/IEC 19790, *Security Requirements for Cryptographic Modules*, on March 1, 2006, and ISO/IEC 24759, *Test Requirements for Cryptographic Modules*, on July 1, 2008. ISO/IEC 19790 specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information



in computer and telecommunication systems. These efforts bring consistent testing of cryptographic modules to the global community by providing ISO-equivalent standards representing FIPS 140-2, *Security Requirements for Cryptographic Modules* and *Derived Test Requirements [DTR]* for FIPS 140-2, *Security Requirements for Cryptographic Modules*.

ISO/IEC JTC 1/SC 27 Working Group (WG) 3 completed and published revisions of ISO/IEC 19790:2006 and ISO/IEC 24759:2008, for which Mr. Randall J. Easter of CSD was the principal editor. The revision of ISO/IEC 19790 was published on August 15, 2012. The revision of ISO/IEC 24759 was published on January 31, 2014. Both ISO/IEC standards were also adopted by the American National Standards Institute (ANSI). The two ISO/IEC revisions were developed with international support and the collaboration of governments, industry and academia. Revised corrections of both standards were published on December 15, 2015.

The revision of ISO/IEC 19790:2012 addresses new security areas such as: defined software module boundaries; degraded modes of operation; trusted channels; two-factor authentication; software security; mitigation of fault induction and side-channel attacks; operational self-tests for algorithms; and life-cycle assurance from design to end-of-life. Figure 2 is a chart of the ISO/IEC standards, as explained above, in which CSD has played a part during the development process.

In addition to the aforementioned standards, the Technical Standard (TS) ISO/IEC TS 30104:2015, *Physical Security Attacks, Mitigation Techniques and Security Requirements*, for which Mr. Easter was the editor, was published on May 15, 2015.

Physical security mechanisms are employed by cryptographic modules where the protection of the module's sensitive security parameters are desired. ISO/IEC 30104 addresses how to express security assurance for products where the risk of the security environment requires the support of such mechanisms. This Technical Specification addresses the following topics:

- A survey of physical security attacks directed against different types of hardware embodiments, including a description of known physical attacks, ranging from simple attacks that require minimal skill or resources, to complex attacks that require trained, technical people and considerable resources;
- Guidance on the principles, best practices and techniques for the design of tamper protection mechanisms and methods for the mitigation of those attacks; and
- Guidance on the evaluation or testing of hardware tamper protection mechanisms and references to current standards and test programs that address hardware tamper evaluation and testing.

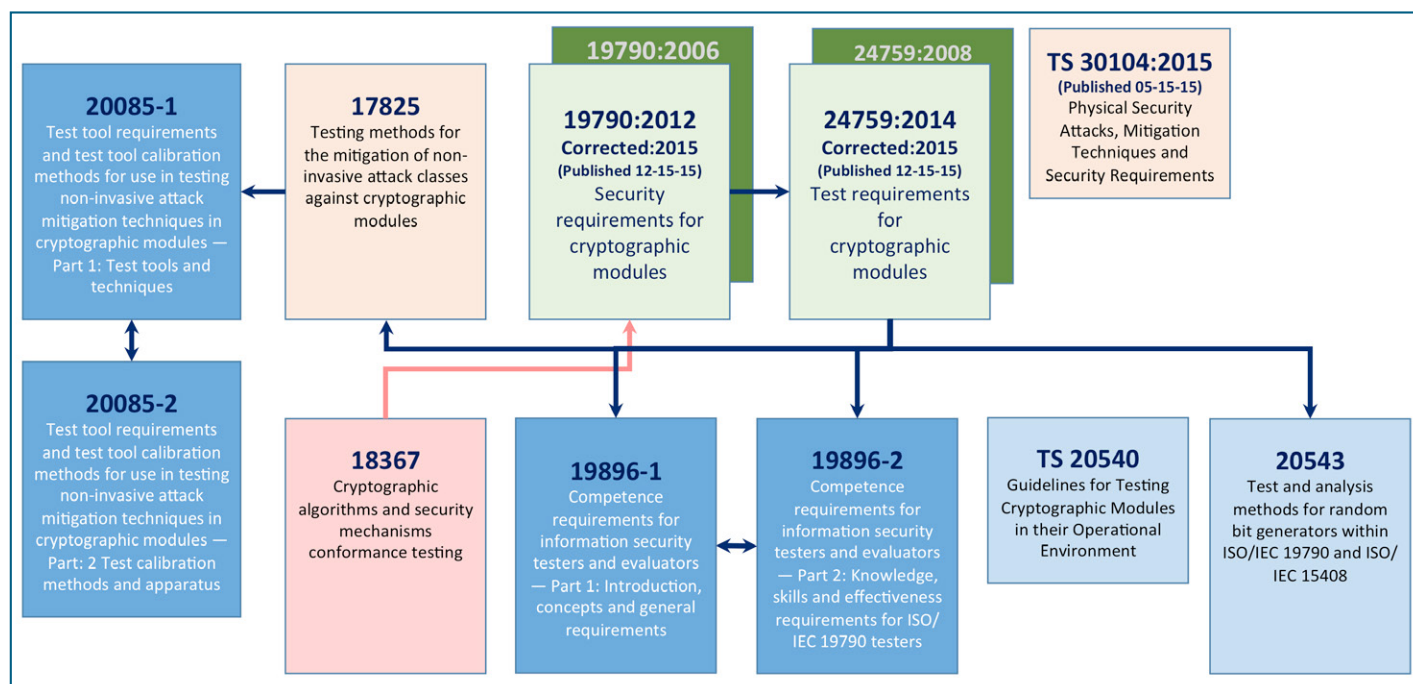


Figure 2: Cryptographic Module Testing – ISO Standards

CSD's Mr. Easter is also the principal editor or co-editor of the following draft ISO/IEC documents:

- ISO/IEC 17825, *Testing methods for the mitigation of non-invasive attack classes against cryptographic modules* (expected publication January 2016);
- ISO/IEC 18367, *Cryptographic algorithms and security mechanisms conformance testing*;
- ISO/IEC 19896-1: *Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements*;
- ISO/IEC 19896-2: *Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers*;
- ISO/IEC 20085-1: *Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques*;
- ISO/IEC 20085-2: *Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 2 Test calibration methods and apparatus*;
- ISO/IEC 20540: *Guidelines for testing cryptographic modules in their operational environment*; and
- ISO/IEC 20543: *Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408*.

CSD's contributions to the development of these international standards create a strong foundation for the adoption of and migration from currently used national standards. In particular, this adoption will promote international harmonization for the implementation and testing of cryptographic algorithms and modules, while accommodating individual country preferences in the choice of approved security functions. CSD published a Federal Register notice in August 2015 seeking public comment for migrating from FIPS 140-2 to ISO/IEC 19790:2012. The comment period ended September 2015 (see <https://federalregister.gov/a/2015-19743>).

#### **For More Information, See:**

<http://csrc.nist.gov/groups/STM/>

#### **CONTACT:**

Mr. Randall J. Easter  
(301) 975-4641  
[randall.easter@nist.gov](mailto:randall.easter@nist.gov)

## **FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) IMPLEMENTATION PROJECT**

The FISMA Implementation Project focuses on:

- Developing a comprehensive series of standards and guidelines to help federal agencies build effective information security programs, defend against increasingly sophisticated cyber-attacks, and demonstrate compliance to security requirements set forth in legislation, Executive Orders, Homeland Security Directives, and Office of Management and Budget (OMB) policies;
- Building a common understanding and reference guides for organizations applying the NIST suite of standards and guidelines that support the NIST Risk Management Framework (RMF) (see <http://csrc.nist.gov/groups/SMA/fisma/framework.html>);
- Developing minimum criteria and guidelines for recognizing security-assessment organization providers as capable of assessing information systems consistent with NIST standards and guidelines supporting the RMF; and
- Conducting FISMA outreach to public and private-sector organizations.

During FY 2015, the CSD FISMA Implementation project continued to strengthen collaboration through the Joint Task Force (JTF) Transformation Initiative, which includes the Department of Defense (DOD), the Intelligence Community (IC), and the Committee on National Security Systems (CNSS), and other federal agencies. The JTF partners continue to develop and update key cybersecurity guidelines for protecting federal information and information systems as part of the Unified Information Security Framework. Previously, the JTF developed common security guidance in the critical areas of security controls for information systems and organizations, security assessment procedures to demonstrate security control effectiveness, security authorizations for risk acceptance decisions, and continuous monitoring activities to ensure that decision makers receive the most up-to-date information on the security state of their information systems. In addition, CSD worked with the General Services Administration (GSA) Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The team developed a high-impact security control baseline

overlay for FedRAMP cloud systems in accordance with NIST standards and guidelines.

In FY 2015, the CSD FISMA Implementation project staff worked on the following initiatives:

- **Risk Management Guidelines:** SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides organizations with the security controls necessary to appropriately strengthen their information systems and the environments in which those systems operate, and provides a process for selecting the appropriate controls, which contributes to systems that are resilient in the face of attacks and other threats. This “Build It Right” strategy is reinforced with the ongoing work on the Second Public Draft of SP 800-160, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*. The implementation of SPs 800-53 and 800-160, combined with the implementation of SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and SP 800 137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, provide organizations with near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions.
- **Guidelines for a Role-Based Information Security Training Model:** SP 800 16, *A Role-Based Model for Federal Information Technology/Cybersecurity Training*, describes a process for developing information technology/cybersecurity role-based training. Its primary focus is to provide a comprehensive, yet flexible, methodology for the development of training courses or modules for personnel who have been identified as having significant information technology/cybersecurity responsibilities within agencies. Agencies can use SP 800-16 to tailor the Role-Based Security Training to meet the needs of their own organization.
- **FISMA Outreach Activity to Public and Private Sector Organizations:** Cybersecurity outreach briefings were conducted and support provided to all levels of government (federal, state and local), as well as private sector organizations, on multiple information security topics of interest. These include, for example, effective implementation of the NIST RMF, contingency planning, interconnection security agreements, and information security for small businesses. In addition, the CSD FISMA implementation project staff conducted outreach activities with academic institutions, providing information on NIST’s security standards and guidelines, exploring

new areas of cybersecurity research and development, and serving on cybersecurity advisory panels.

- **Collaboration with JTF partners and other federal organizations:** CSD staff worked closely with JTF partners on continued cooperation and planning to ensure that the five JTF publications remain current, and on the designation of additional special publications as JTF guidance. The CSD FISMA implementation project staff also collaborated with DOD, IC, the Department of Homeland Security (DHS), the Federal Emergency Management Agency (FEMA), the Government Accountability Office (GAO), OMB, GSA, the Small Business Administration (SBA), and the Inspector Generals (IGs) on multiple projects to ensure consistency with FISMA-related guidance and to protect information in a way that is commensurate with risk.

In FY 2015, the CSD FISMA Implementation project staff completed the following activities:

- Published the final version of SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*;
- Published both Initial Public Draft (IPD) and final versions of SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, to provide guidance to federal agencies for the protection of Controlled Unclassified Information when such information is resident in nonfederal information systems and organizations;
- Published an errata version of SP 800-53, Revision 4 to make necessary clarifications and ensure consistency with subsequently published/revised NIST SPs and new/updated federal policy requirements;
- Continued collaboration with DHS to develop a multiple-volume *Interagency Report on Automation Support for Ongoing Assessments*, which is based on NIST standards and guidelines; and
- Continued the development of preliminary drafts of SP 800-18 Revision 2, *Guide for Developing Security Plans for Federal Information Systems and Organizations* and SP 800-60 Revision 2, *Guide for Mapping Types of Information and Information Systems to Security Categories*.

In FY 2016, CSD FISMA Implementation project staff intend to:

- Finalize SP 800-160, *Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*;



- Finalize SP 800-16, *A Role-Based Model for Federal Information Technology / Cybersecurity Training*;
- Begin the development of SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*;
- Continue to explore ways to use automation to support SP 800-53 updates;
- Continue the development of SP 800-60, Revision 2, *Guide for Mapping Types of Information and Information Systems to Security Categories*;
- Continue the development of SP 800-18, Revision 2, *Guide for Developing Security Plans for Federal Information Systems and Organizations*;
- Expand cybersecurity outreach to include additional state, local, and tribal governments, as well as private sector organizations and academic institutions;
- Continue to support federal agencies in the effective implementation of the RMF; and
- Continue collaboration with JTF partners and other federal organizations.

**For More Information, See:**

<http://csrc.nist.gov/groups/SMA/fisma>

**CONTACTS:**

Dr. Ron Ross  
(301) 975-5390  
[ron.ross@nist.gov](mailto:ron.ross@nist.gov)

Ms. Pat Toth  
(301) 975-5140  
[patricia.toth@nist.gov](mailto:patricia.toth@nist.gov)

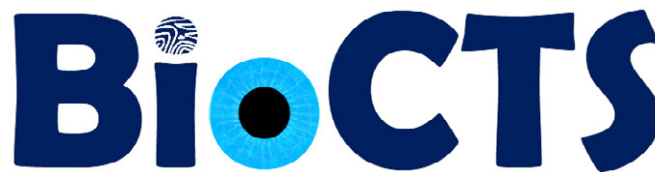
Ms. Kelley Dempsey  
(301) 975-2827  
[kelley.dempsey@nist.gov](mailto:kelley.dempsey@nist.gov)

Ms. Peggy Himes  
(301) 975-2489  
[peggy.himes@nist.gov](mailto:peggy.himes@nist.gov)

## BIOMETRIC STANDARDS AND ASSOCIATED CONFORMITY ASSESSMENT TESTING TOOLS

NIST's CSD supports the development of biometric conformance testing methodology standards and other conformity-assessment efforts through active technical participation in the development of these standards and the development of associated conformance test software, architectures and test suites. These test tools are developed to promote the adoption of these standards and to support users that require conformance to selected biometric standards, product developers and testing labs.

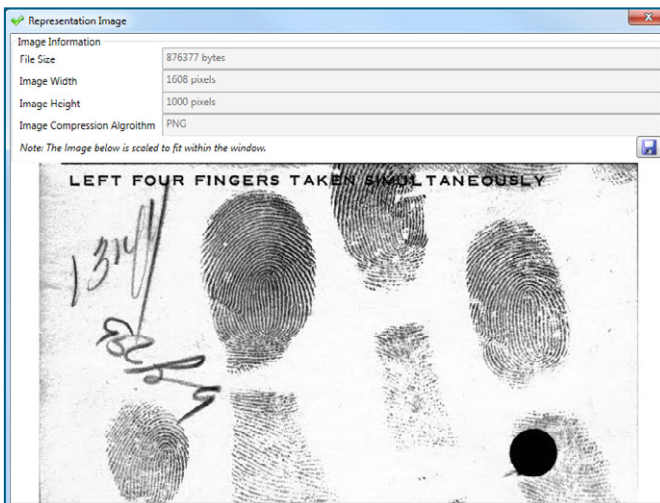
CSD's project team contributes to the development of biometric standards and participates in the INCITS Technical Committee M1 – *Biometrics* and ISO/IEC Joint Technical Committee (JTC) 1 Subcommittee (SC) 37 – *Biometrics* standards bodies. CSD plans to continue this work in FY 2016.



In FY 2015, Biometric Conformance Test Software (BioCTS) for ANSI/NIST-ITL (which targets biometric transactions based on NIST SP 500-290, and SP 500-290 Revision 1 - *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*) received a substantial update. Version 2.0 of the testing software was released and added support for testing for the remaining traditionally encoded record types not previously supported (+12 for ANSI/NIST-ITL 1-2011, and +18 for ANSI/NIST-ITL 1-2011 Update: 2013). Version 2.0 now supports all traditionally encoded biometric record types between the two versions of the published ANSI/NIST-ITL standards. Additionally, Version 2.0 added many enhanced editing features for traditionally encoded biometric transactions – some new features include: adding and removing records and fields, arranging records and fields, automatically sorting records, displaying the biometric sample image, and enhanced binary data editing features. In addition to the enhanced editing features, BioCTS for ANSI/NIST-ITL received many usability enhancements, as well as updates to some core software functionality, providing a more usable and robust testing tool.

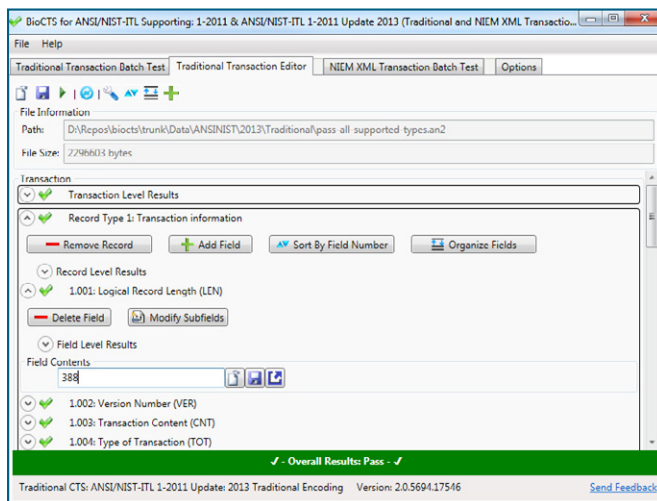
As illustrated in Figure 3, a new feature of BioCTS is the display of the biometric sample, when possible, so that the user can get visual feedback on the biometric data that is under test. The update provides a rich editing environment for binary/traditionally encoded transactions and files, which are difficult for humans to read. Version 2.0 provides a user-friendly way to see each field within a transaction/file, associated test results, and allows for the modification of data (as shown in Figure 4.) All of the new features are detailed in the *BioCTS for ANSI/NIST-ITL v2 User Guide* (see: [http://csrc.nist.gov/groups/ST/BiomResCenter/CTA\\_BETA/BioCTS\\_AN\\_ITL\\_v2\\_Guide.pdf](http://csrc.nist.gov/groups/ST/BiomResCenter/CTA_BETA/BioCTS_AN_ITL_v2_Guide.pdf)).





**Figure 3: BioCTS displays the biometric sample to provide visual feedback.**

The latest version of BioCTS was released in August 2015, together with documentation and sample data. The BioCTS software installer files, as well the ancillary tools and sample data can be downloaded from the NIST Biometrics website. (see: [http://www.nist.gov/itl/csd/biometrics/biocta\\_download.cfm](http://www.nist.gov/itl/csd/biometrics/biocta_download.cfm)).



**Figure 4: BioCTS provides a rich editing environment for reviewing and updating records.**

A number of technical contributions towards the development of ANSI/NIST and international standards were submitted. They included technical contributions on international biometric data interchange formats and their associated conformance testing methodologies, as well as on SP 500-290 Revision 1 and the associated National Information Exchange Model (NIEM) Extensible Markup Language (XML) Schema (see <https://tools.niem.gov>).

Outreach efforts in FY 2015 in support of biometric standards development and conformity assessment included test tool contributions for the standards developers (in support of ongoing development projects), and presentations on ANSI/NIST and international biometric standards and related conformity assessment activities. The work included the development of technical publications, the review of research papers for external publications, and participation in conference program committees. CSD published NIST Special Publication 500-304, *Conformance Testing Methodology Framework for ANSI/NIST-ITL 1-2011 Update: 2013, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information* in June 2015. Additionally, CSD published NIST SP 500-304 Annex D: *Test Notes and Exceptions for the ANSI/NIST ITL 1-2011 Update 2013 Conformance Testing Methodology Framework* in July 2015.

#### **For More Information, See:**

BioCTS - Biometric Conformance Test Tool Downloads:

[http://www.nist.gov/itl/csd/biometrics/biocta\\_download.cfm](http://www.nist.gov/itl/csd/biometrics/biocta_download.cfm)

NIST Special Publication 500-304: *Conformance Testing Methodology Framework for ANSI/NIST-ITL 1-2011 Update: 2013, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-304.pdf>

NIST SP 500-304 Annex D: Test Notes and Exceptions for the ANSI/NIST ITL 1-2011 Update 2013 Conformance Testing Methodology Framework:

[http://csrc.nist.gov/groups/ST/BiomResCenter/CTA\\_BETA/External\\_Notes\\_Exceptions\\_NIST\\_SP\\_500\\_304\\_with\\_Errata.pdf](http://csrc.nist.gov/groups/ST/BiomResCenter/CTA_BETA/External_Notes_Exceptions_NIST_SP_500_304_with_Errata.pdf)

#### **CONTACT:**

Mr. Dylan Yaga  
(301) 975-6004  
[dylan.yaga@nist.gov](mailto:dylan.yaga@nist.gov)

## SECURITY OF CYBER-PHYSICAL SYSTEMS (CPS)

CSD's overall Cyber-Physical Systems (CPS) effort will provide the next generation of "smart," co-designed and co-engineered interacting networks of physical and computational components. Specifically, CSD supports the effort by providing cybersecurity and privacy experts who help leverage existing resources and address CPS-specific cybersecurity and privacy challenges. Such challenges are related to personalized health care, emergency response, traffic flow management, and electric power generation and delivery, and many other emerging technical areas. Other phrases that are often referenced along with CPS technologies include:

- Internet of Things (IoT);
- Industrial Internet;
- Smart Cities;
- Smart Grid; and
- "Smart" Anything (e.g., Cars, Buildings, Homes, Manufacturing, Hospitals, Appliances) (see <http://www.nist.gov/cps/>).

Composed of heterogeneous, potentially distributed components and systems, CPS provides a promise of increased efficiency and interaction between the digital and physical worlds. However, assuring that these emerging and evolving systems are reliable, robust, resilient, trustworthy, secure, and that they protect the privacy of information (to only list a few concerns) poses a unique cybersecurity challenge.

CPS present unique challenges, including the need for integration with legacy components and allowance for emerging technologies, and real-time response in support of extremely high availability, predictability, and reliability.

Cybersecurity is an important crosscutting discipline that is critical to the safe and resilient design, development and operation of CPS. Addressing the opportunities and challenges of CPS requires a broad collaboration to develop a common foundation, including a consensus definition, vocabulary, reference architecture, and a shared understanding of the essential roles of timing, cybersecurity and data interoperability. CSD is researching the cybersecurity needs of the broader landscape of CPS by leveraging CSD's expertise in cybersecurity in different domains and applications of CPS (such as industrial control systems, the smart grid, hardware-enabled security, and embedded systems).

In June 2014, NIST established the CPS Public Working Group (PWG), which is open to all, to foster and capture inputs from those involved in CPS, both nationally and globally. CSD is working in collaboration with NIST's Engineering Laboratory (EL) Smart Grid and Cyber-Physical Systems Program Office, NIST's Physical Measurement Laboratory Time and Frequency Division, ITL's Software and Systems Division and ITL's Advanced Networking Technologies Division to lead a working group of government, academic, and industry stakeholders. The CPS PWG consists of five technical subgroups:

- Definition, Vocabulary, and Reference Architecture;
- Use Cases;
- Cybersecurity and Privacy;
- Data Interoperability; and
- Timing and Synchronization.

Each subgroup consists of co-leaders from academia, industry and NIST. CSD co-leads the Cybersecurity and Privacy subgroup that is focused on identifying strategies for cybersecurity and privacy in CPS, and is working collaboratively with the other subgroups to ensure that cybersecurity is included as a design principle during development.

In September 2015, the CPS PWG published the *Draft Framework for CPS* that includes the work of the five technical subgroups. The document reflects more than a year's effort by the CPS PWG, which includes a few hundred members drawn primarily from industry, academia and government. In 2016, the CPS PWG will collect and analyze the comments to the draft and publish the next version of the CPS Framework. The CPS PWG deliverables are technology and business-model neutral, and freely available online and intended for open use by all stakeholders.

Additionally, in 2015, CSD, in conjunction with NIST's Engineering Laboratory, Intelligent Systems Division, finalized SP 800-82 Revision 2, *Guide to Industrial Control Systems Security*. CSD will also continue to participate in the International Society of Automation (ISA) 99 Committee, which develops and establishes standards, recommended practices, technical reports, and related information that define procedures for implementing electronically secure industrial automation and control systems and security practices, and for assessing electronic security performance.

### For More Information, See:

<http://www.nist.gov/cps/>

## CONTACTS:

Mr. Stephen Quinn      Ms. Suzanne Lightman  
(301) 975-6967      (301) 975-6442  
stephen.quinn@nist.gov      suzanne.lightman@nist.gov

## FEDERAL CYBERSECURITY RESEARCH & DEVELOPMENT (R&D)

The Networking and Information Technology Research and Development (NITRD) program provides a framework in which many federal agencies come together to coordinate their networking and IT research and development (R&D) efforts. CSD remained committed to the value of communicating its R&D efforts to other federal colleagues and identifying the opportunities to support R&D efforts throughout the Federal Government.

In FY 2015, the NITRD Cyber Security and Information Assurance (CSIA) Interagency Working Group (IWG) monthly meetings provided an opportunity to learn and share information about NIST's ongoing research with federal program managers of cybersecurity research (see [https://www.nitrd.gov/nitrdgroups/index.php?title=Cyber\\_Security\\_and\\_Information\\_Assurance\\_Interagency\\_Working\\_Group\\_\(CSIA\\_IWG\)#title](https://www.nitrd.gov/nitrdgroups/index.php?title=Cyber_Security_and_Information_Assurance_Interagency_Working_Group_(CSIA_IWG)#title)). The Cybersecurity Enhancement Act of 2014 requested the development of a new federal cybersecurity research and development strategic plan, and NIST was a consistent presence at the regular development meetings for the new plan that is intended for release during the month of February 2016. (see Cybersecurity Enhancement Act of 2014 <https://www.congress.gov/bill/113th-congress/senate-bill/1353/text>, and see strategic plan [https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016\\_Federal\\_Cybersecurity\\_Research\\_and\\_Development\\_Strategic\\_Plan.pdf](https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Strategic_Plan.pdf)).

FY 2015 also included the development of a National Privacy Research Strategy by the members of the National Privacy Research Forum (see <https://www.nitrd.gov/cybersecurity/nationalprivacyresearchstrategy.aspx>). Naomi Lefkowitz, Senior Privacy Policy Advisor at NIST, and Simson Garfinkel, Senior Advisor in the Information Access Division, shared NIST's focus on privacy and brought their expertise to the development process for the privacy R&D plan that will be published in FY 2016.

NIST regularly attended the NITRD CSIA Senior Steering Group meetings to share and stay connected with opportunities that supported the development of the new

strategic plan for cybersecurity R&D and participated in panel presentations to which the SSG was invited to describe federal directions in cybersecurity R&D at relevant forums and conferences (see [https://www.nitrd.gov/nitrdgroups/index.php?title=Cyber\\_Security\\_Information\\_Assurance\\_Research\\_and\\_Development\\_Senior\\_Steering\\_Group\\_\(CSIA\\_R%26D\\_SSG\)#title](https://www.nitrd.gov/nitrdgroups/index.php?title=Cyber_Security_Information_Assurance_Research_and_Development_Senior_Steering_Group_(CSIA_R%26D_SSG)#title)).

CSD is also a regular participant in the coordination activities of the federal Special Cyber Operations Research and Engineering (SCORE) Committee. SCORE enables technology transfer through the sharing of NIST cybersecurity expertise and publications with researchers throughout the Federal Government. The SCORE committee interacts with federal leaders and reports to the National Science & Technology Council's Committee on Homeland & National Security. In FY 2015, NIST expertise in supply chain risk management and cryptography was included in SCORE reports.

### For More Information, See:

<http://www.nitrd.gov/>

## CONTACT:

Mr. Bill Newhouse  
(301) 975-2869  
william.newhouse@nist.gov

## SECURITY ASPECTS OF ELECTRONIC VOTING

In 2002, Congress passed the Help America Vote Act (HAVA) to encourage the upgrade of voting equipment across the United States. HAVA established the Election Assistance Commission (EAC) and the Technical Guidelines Development Committee (TGDC), chaired by the Director of NIST. HAVA directs NIST to provide technical support to the EAC and TGDC in efforts related to human factors, security, and laboratory accreditation. As part of NIST's efforts, CSD supports the activities of the EAC related to voting equipment security.

In the past year, NIST continued to support the EAC in finalizing changes to the Voluntary Voting System Guidelines (VVSG) 1.1. These changes sought to improve the auditability of voting systems, provide greater software integrity protections, expand and improve access-control requirements, and help ensure that cryptographic security mechanisms are implemented properly. The EAC approved these updates to the VVSG in March 2015. In addition, NIST completed a set of draft test assertions for the security requirements in the VVSG. This included test assertions in the



areas of access control, software setup and validation, polling place security, and the use of public telecommunications networks.

Initial efforts on the next-generation of the VVSG have already begun. In February, NIST and the EAC sponsored the second Future of Voting Systems Symposium. This symposium brought together election officials, voting system manufacturers, voting system test laboratories, standards developers, academics, and federal, state, and local government officials to discuss emerging trends in voting. The discussions at this workshop are being used to define the scope and priorities for the next-generation guidelines.

In FY 2016, NIST and the EAC will establish a set of public working groups to inform the development of a new version of the VVSG. NIST and EAC goals are to accelerate the development and adoption of the VVSG by leading these working groups in close consultation with election officials, the federal and private sectors, standards bodies and EAC committees, academic researchers, and other members of the public. These working groups will focus on voting system technology areas, including accessibility, usability, interoperability, security, and testing and certification.

**For More Information, See:**

<http://vote.nist.gov>

**CONTACTS:**

Mr. Andrew Regenscheid  
(301) 975-5155  
[andrew.regenscheid@nist.gov](mailto:andrew.regenscheid@nist.gov)

Mr. Joshua Franklin  
(301) 975-8463  
[joshua.franklin@nist.gov](mailto:joshua.franklin@nist.gov)

## HEALTH INFORMATION TECHNOLOGY SECURITY

Health Information Technology (HIT) enables better patient care through the secure use and sharing of health information. HIT leads to improvements in healthcare quality, reduced medical errors, increased efficiencies in health care delivery and administration, and improved health for the general population. Central to reaching these goals is the assurance of the confidentiality, integrity, and availability of health information. CSD works with government, industry, academia, and others to provide security tools, technologies, and methodologies that provide for the security and privacy of health information.

NIST CSD continued its HIT security outreach efforts in FY 2015. NIST and the Department of Health and Human

Services' (DHHS) Office for Civil Rights (OCR) co-hosted the eighth annual Health Insurance Portability and Accountability Act (HIPAA) Security Rule conference, *Safeguarding Health Information: Building Assurance through HIPAA Security*, in September 2015 in Washington, D.C. The conference offered important sessions that focused on broad topics of interest to the healthcare and health IT security community. Over 600 in-person and virtual attendees from federal, state, and local governments, academia, HIPAA-covered entities and business associates, industry groups, and vendors heard from, and interacted with, healthcare, security, and privacy experts on technologies and methodologies for safeguarding health information and for implementing the requirements of the HIPAA Security Rule. Presentations and panel discussions covered a variety of security management and technical assurance topics, including:

- Collaborative approaches for securing medical devices;
- Vulnerabilities in medical devices and control systems;
- Business associate liability;
- Information sharing and threat intelligence;
- Data recovery and security plans; and
- Securing electronic health records on mobile devices.

The keynote addresses were delivered by Jocelyn Samuels, Director, DHHS/OCR, and Dr. Cris Ewell, Chief Information Security Officer at Seattle Children's Hospital.

In FY 2016, NIST will work with diverse healthcare stakeholders, including partners in government and industry, to support security capabilities in new areas, such as the Precision Medicine Initiative, and identify opportunities to strengthen the sector's cybersecurity risk management efforts through the application of the NIST Cybersecurity Framework.

**For More Information, See:**

<http://www.nist.gov/healthcare/security/>

**CONTACT:**

Mr. Kevin Stine  
(301) 975-4483  
[kevin.stine@nist.gov](mailto:kevin.stine@nist.gov)



## SUPPLY CHAIN RISK MANAGEMENT (SCRM) FOR INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT)

Information and communication technologies have rapidly become more numerous and more capable. These technologies increasingly rely on a supply-chain ecosystem that is long, complex, variable, interconnected, globally distributed, and geographically diverse. Outsourcing the development, maintenance, management, and disposal of data and ICT is increasingly common.

These trends have caused organizations acquiring technology to experience a lack of visibility throughout the supply chain (see Figure 5). Such organizations need a better understanding of how the technology being acquired was developed, integrated and deployed. These organizations also need to better understand the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services being obtained. This lack of visibility and understanding, in turn, has decreased the acquiring organization's ability to effectively manage risk inherited from the supply chain.

The Supply Chain Risk Management (SCRM) program seeks to provide organizations with a standardized and repeatable toolkit of technical and intelligence resources to strategically manage supply-chain risk throughout the entire lifecycle of systems, products and services.

In FY 2015, CSD finalized and published NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*. This document builds on existing NIST guidance to help federal departments and agencies identify, assess and mitigate ICT supply-chain risk at all organizational levels.

When NIST researched and developed the *Framework for Improving Critical Infrastructure Cybersecurity*, which was published in February 2014, cyber supply-chain risk management (CSCRM) was identified as an area needing further research and guidance (see the *NIST Roadmap for Improving Critical Infrastructure Cybersecurity*, also published in February 2014). In FY 2015, CSD initiated a project on industry best practices for CSCRM. Initial research was developed into company case studies spanning multiple business sectors. The studies will be analyzed to support a workshop, and a final publication is planned for FY 2016.

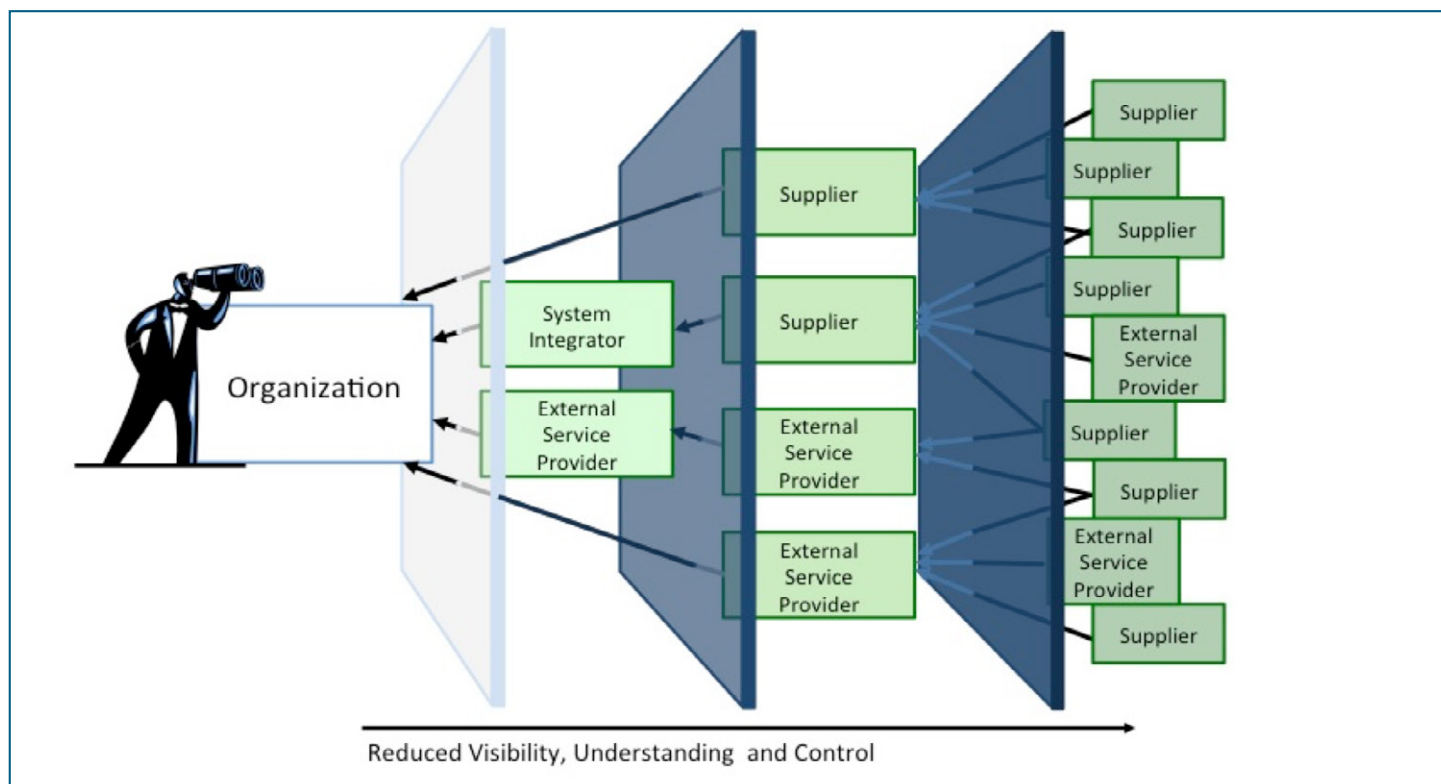


Figure 5: Visibility Challenges for Supply Chain Risk Management (SCRM)

CSD staff continued to join staff members from the Department of Defense in co-chairing a U.S. federal interagency working group on SCRM. The working group evolved from the White House's Comprehensive National Cybersecurity Initiative (CNCI) 11, *Develop a Multi-Pronged Approach for Global Supply Chain Risk Management*, which ended in 2014. In FY 2015, the co-chairs began the process of formalizing the working group under the auspices of the CNSS.

CSD continued working with partners through the Software and Supply Chain Assurance (SSCA) Forum, co-sponsoring four multi-day workshops. The SSCA Working Group (WG) is a key public-private partnership that meets quarterly to discuss current projects, tools, resources, and lessons learned regarding CSCR. The SSCA WG is co-sponsored by NIST, GSA, DoD and DHS.

In FY 2016, CSD will:

- Continue working on Industry Best Practices for Cyber Supply Chain Management, including hosting a two-day workshop, developing cyber supply-chain standards mappings to the Cybersecurity Framework, as well as a strategy to better integrate the supply-chain management and information security functions in organizations; the various pieces of the research project will culminate in a draft guidance document;
- Continue to co-chair the interagency working group on cyber supply-chain risk management;
- Begin research to demonstrate cause and effect relationships between cyber supply-chain capability/maturity levels and organizational performance outcomes over time; and
- Research metrics for use in supply chain risk management.

#### For More Information, See:

<http://csrc.nist.gov/scrm/>

## CONTACTS:

ICT SCRM Team email: [scrm-nist@nist.gov](mailto:scrm-nist@nist.gov)

Mr. Jon Boyens  
Program Lead  
(301) 975-5549  
[jon.boyens@nist.gov](mailto:jon.boyens@nist.gov)

Ms. Celia Paulsen  
Technical Lead  
(301) 975-5981  
[celia.paulsen@nist.gov](mailto:celia.paulsen@nist.gov)

## NATIONWIDE PUBLIC SAFETY BROADBAND NETWORK (NPSBN) CYBERSECURITY



Source: <http://www.pscr.gov/>

In February 2012, Congress passed the Middle Class Tax Relief and Job Creation Act. One portion of this legislation calls for the establishment of a nationwide, interoperable public-safety broadband network based on the 3rd Generation Partnership Project's (3GPP) Long-Term Evolution (LTE) technology. The network will be deployed and operated by the First Responder Network Authority (FirstNet). The planned NPSBN will *"create a much needed nationwide interoperable broadband network that will help police, firefighters, emergency medical service professionals and other public safety officials stay safe and do their jobs."* (see <http://www.ntia.doc.gov/category/public-safety>). NIST is directed to establish a list of certified devices and required components to be used by public-safety officials, vendors, and other interested parties for interacting with the nationwide network. NIST is also directed to conduct research and development that supports the acceleration and advancement of the nationwide network.

In FY 2015, CSD supported the joint National Telecommunications and Information Administration (NTIA) and NIST Public Safety Communications Research (PSCR) program with efforts in public-safety mobile-application security, identity management, and enabling cybersecurity capabilities on the PSCR 700 MHz LTE network located in Boulder, Colorado (see <http://www.pscr.gov>). In June 2015, CSD, in cooperation with the Association of Public-Safety Communications Officials (APCO) International and FirstNet, held a half-day workshop titled *"Identifying and Categorizing Data Types for Public Safety Mobile Applications."* The outcome of that workshop will be captured in a forthcoming NIST publication in FY 2016. At PSCR's Annual Public Safety Broadband Stakeholder Conference, CSD organized a panel titled "Applied Public Safety Cybersecurity Research" highlighting PSCR's cybersecurity activities over the previous twelve months in the areas of identity management, mobile application security, and LTE infrastructure cybersecurity.

During FY 2015, CSD published NISTIR 8018, *Public Safety Mobile Application Security Requirements*

Workshop Summary, and NISTIR 8014, *Considerations for Identity Management in Public Safety Mobile Networks*. In addition, CSD developed an informational survey on mobile application vetting services titled “*Mobile Application Vetting Services for Public Safety*” and Draft NISTIR 8080, *Usability and Security Considerations for Public Safety Mobile Authentication*.

CSD participated in the standards development process for LTE technology within the 3GPP, supporting security requirements for public safety that are related to Proximity Services (ProSe), Group Communication System Enablers (GCSE), and Mission Critical Push-To-Talk (MCPTT). In addition, CSD broadened its scope within the IETF to include efforts related to public safety.

In FY 2016, CSD will continue representing public safety in international standardization efforts, such as the IETF and 3GPP. CSD will work to implement and exercise LTE cybersecurity infrastructure capabilities in the PSCR 700 MHz LTE network, conduct research into mobile authentication solutions to support public-safety, and investigate mobile application-security services and solutions to support the security requirements of public-safety mobile applications and devices. CSD will continue to engage the public-safety communications community by organizing workshops and conferences; and participating in events such as APCO’s Annual Meeting, PSRC’s Annual Public Safety Broadband Stakeholder Conference, and the International Wireless Communications Expo (IWCE).

## CONTACTS:

Ms. Sheila Frankel  
(301) 975-3297  
sheila.frankel@nist.gov

Dr. Nelson Hastings  
(301) 975-5237  
nelson.hastings@nist.gov

## SMART GRID CYBERSECURITY

The major elements of the smart grid are information technology, industrial control systems/operational technology and the communications infrastructure. The infrastructure is used to send command information across the electric grid from generation systems to distribution systems, and to exchange usage and billing information between utilities and their customers. Key to the successful deployment of the smart grid infrastructure is the development of the cybersecurity strategy that includes cybersecurity as a design consideration for new and emerging systems, and an approach to adding cybersecurity into existing systems. The electric grid is critical to the economic and physical well-being of the nation, and emerging cyber threats targeting power systems highlight



the need to integrate advanced security to protect critical assets.

The Smart Grid Interoperability Panel (SGIP) became a membership-supported organization in January 2013. The SGIP Cybersecurity Working Group (CSWG) was renamed the Smart Grid Cybersecurity Committee (SGCC), and continues to be led by Ms. Suzanne Lightman of the CSD in support of responsibilities identified in the Energy Independence and Security Act of 2007. The SGCC chair is a voting member of the SGIP Technical Committee, and serves as an ex-officio Director of the Board.

During the last year, staff from CSD and ITL’s Software and Systems Division (SSD) worked on developing network security tools that are specifically designed to support next-generation electrical power systems. They concentrated on authenticating the provenance of multicast data streams from emerging power system sensors, called Phasor Measurement Units. By authenticating the sensors to the utility, the utility may trust that sensor measurements are coming from the correct sensors and have not been hijacked.

Multicast authentication of sensor data is challenging, due to the need for low security overhead, tolerance of lossy networks, time-criticality, and high data rates. Researchers augmented an existing authentication scheme to accommodate high-data-rate sensor transmissions that are unbounded in length (no session expiration). Using dual offset key chains to reduce the authentication delay and computational overhead associated with key chain commitment, they developed a new protocol called *inf-TESLA* that meets the performance requirements imposed by the physical dynamics of the power system.

Their key disclosure mechanism, as well as comparative studies showing a cumulative reduction in the communication overhead and computational cost over existing methods, are outlined in a paper to appear at the Association for Computing Machinery (ACM) Symposium on Applied Computing.

Significant effort was made to integrate their authentication protocol into existing network simulation software, specifically OPNET, thus providing potential users the ability to evaluate the protocol on their own networks and for their own applications.

Furthermore, in an effort to address the growing interest in co-optimizing cyber and physical components to work together as a system, CSD staff developed mathematical formalism to tradeoff the sensitivity of a dynamic system to attack or perturbation against the authentication overhead incurred by their protocol. This formalism was



demonstrated on a power system use case showing the limiting considerations between authentication overhead and stability margins of a wide-area damping controller.

In FY 2016, CSD will coordinate with NIST's Engineering Laboratory (EL) and Smart Grid Program Office on the further development of a Cybersecurity Smart Grid Test Lab, part of the NIST Smart Grid Testbed Facility now under construction. CSD will also collaborate with SSD on cybersecurity research in relation to the IEEE 1588, Precision Time Protocol, a time synchronization standard that is used for the electric grid and other special-purpose industrial automation and measurement networks.

#### For More Information, See:

<http://www.nist.gov/smartgrid>

<http://www.sgip.org>

## CONTACTS:

Ms. Suzanne Lightman  
(301) 975-6442  
[suzanne.lightman@nist.gov](mailto:suzanne.lightman@nist.gov)

Ms. Victoria Yan Pillitteri  
(301) 975-8542  
[victoria.pillitteri@nist.gov](mailto:victoria.pillitteri@nist.gov)

Ms. Tanya Brewer  
(301) 975-4534  
[tbrewer@nist.gov](mailto:tbrewer@nist.gov)

## CYBERSECURITY AWARENESS, TRAINING, EDUCATION, AND OUTREACH

### National Initiative for Cybersecurity Education (NICE)

NIST has been the lead for the National Initiative for Cybersecurity Education (NICE) since its inception in 2010. NICE is responsive to President Obama's declaration that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and "America's economic prosperity in the 21st century will depend on cybersecurity."

The NICE program seeks to foster, energize, and promote a robust network and an integrated ecosystem of cybersecurity education, training, and workforce development.

CSD is leading the NICE program, working from the strengths and energy of more than twenty federal departments and agencies, leveraging each of their relationships with academia and industry sectors to ensure

coordination, cooperation, focus, public engagement, technology transfer and sustainability. NIST will highlight these activities, engage various stakeholder groups and create forums for sharing information and leveraging best practices.

The NICE Program Office focuses on the following activities:

- **Accelerate** learning and skills development by invoking a sense of urgency in both the public and private sectors to address the shortage of a skilled cybersecurity workforce;
- **Nurture** a diverse learning community through strengthening education and training across a multifarious ecosystem that prioritizes learning, emphasizes outcomes, and celebrates diversity; and
- **Guide Career Development and Workforce Planning** that supports job seekers and employers in addressing market demands and maximizing talent management.

The NICE Program Office staff promoted NICE activities through contributions to many events, symposia, forums, competitions, educational outreach meetings, and workshops. The staff continued its leadership to achieve the Office of Personnel Management (OPM) Cross-Agency Priority Goal: "Closing Skills Gaps" for the IT/Cybersecurity workforce. The staff focused on reducing cybersecurity workforce gaps and supported the goals of the White House's "Ready to Work" initiative. In addition, the staff took leadership of the NICE Working Group, a group established to provide a mechanism in which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development.

In FY 2015, the NICE Program Office announced that a grant will be awarded to support the development of a visualization tool to show the demand for and availability of critical cybersecurity jobs across the nation. This cybersecurity jobs "heat map" will be developed in partnership with Computing Technology Industry Association (CompTIA) and Burning Glass Technologies. The map will provide data to help employers, job seekers, policy makers, training providers, and guidance counselors in order to meet today's increasing demand for cybersecurity workers. NICE also provided grant support for the NICE 2015 Conference and Expo, the inaugural National Cybersecurity K-12 Cybersecurity Education Conference, the Centers of Academic Excellence (CAE) Community Meeting, and the NICE Challenge Project.

In FY 2016, the NICE Program Office will continue to promote the coordination of existing and future cybersecurity education, training, and workforce activities. The

Sixth annual NICE Workshop will take place on November 3-4, 2015 in San Diego, CA (see <http://csrc.nist.gov/nice/events.html>). NIST will also identify opportunities to extend and integrate the NICE focus on the cybersecurity workforce, education, and training within NIST Special Publications and informational reports, while promoting the value of the National Cybersecurity Workforce Framework (NCWF) and the forthcoming DOD Cyberspace Workforce Strategy as resources that address cybersecurity workforce needs.

**For More Information, See:**

<http://www.nist.gov/nice/>

---

**CONTACTS:**

Mr. Rodney Peterson  
NICE Director  
(301) 975-8897  
[rodney@nist.gov](mailto:rodney@nist.gov)

Ms. Danielle Santos  
NICE Program Manager  
(301) 975-5048  
[danielle.santos@nist.gov](mailto:danielle.santos@nist.gov)

**Computer Security Resource Center (CSRC)**

The CSRC, Computer Security Division's (CSD) website, is one of the most visited websites at NIST. CSRC encourages the broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies and links key security web resources to support industry and government users. CSRC is an integral component of all of the work that CSD conducts and produces. It is CSD's repository for anyone wanting to access these documents and other valuable security-related information. During FY 2015, CSRC had more than 5.9 million page views and downloads.

CSRC is the primary gateway for gaining access to NIST computer security publications, standards, and guidelines, and serves as a vital link to CSD's customers. Publications are organized to help users locate relevant information quickly and are arranged by topic, relevant security control family, and legal requirements.

In addition to CSRC, CSD maintains a publication announcement mailing list. This free e mail list notifies subscribers about publications that have been posted to the CSRC website, along with announcing new CSD-sponsored events and important news and/or announcements. The e-mail list is a valuable tool for more than 59,000 subscribers from the Federal Government, industry, academia, and individuals with a personal interest in IT security worldwide. Individuals who are interested in subscribing to this list should visit <http://csrc.nist.gov/publications/subscribe.html> for more information.

During FY 2015, the CSRC has been updated on a daily basis with new information, such as the publication of draft and final documents (FIPS, SPs, NISTIRs and ITL Bulletins) and various project and program webpage updates. An improvement made to the CSRC homepage was to add a new section titled "Draft Publications Request for Comments Deadlines". This section will help our customers that are interested in submitting comments to our technical publications find the deadline dates for submitting comments to certain publications.

The CSRC website is expected to be redesigned during FY 2016 to provide an improved and flexible user interface.

**For More Information, See:**

<http://csrc.nist.gov>

---

**CONTACTS:**

Questions regarding the CSRC website can be sent to the CSRC Webmasters at: [webmaster-csrc@nist.gov](mailto:webmaster-csrc@nist.gov).

Mr. Patrick O'Reilly  
(301) 975-4751  
[patrick.oreilly@nist.gov](mailto:patrick.oreilly@nist.gov)

Ms. Nicole Keller  
(301) 975-3648  
[nicole.keller@nist.gov](mailto:nicole.keller@nist.gov)

(Editor Note: Ms. Judy Barnard was part of this project team until her recent retirement.)

**Federal Computer Security Managers' (FCSM) Forum**

The Federal Computer Security Managers' (FCSM) Forum is sponsored by NIST to promote the sharing of security-related information among federal agencies. The Forum, which serves more than 1,100 members, strives to provide an ongoing opportunity for managers of federal information security programs to exchange information security materials in a timely manner, build upon the experiences of other programs, and reduce possible duplication of effort. It provides a mechanism for NIST to share information directly with federal agency information security managers in fulfillment of NIST's leadership mandate under FISMA. It assists NIST in establishing and maintaining relationships with other individuals or organizations that are actively addressing information security issues within the Federal Government. CSD's Patricia Toth serves as the Chairperson and Peggy Himes serves as the Secretariat.

The Forum maintains an extensive email subscription service. Participation in the service is only open to Federal Government employees who participate in the management of their organization's information system security

program. The Forum also holds bimonthly meetings and an annual two-day conference to discuss current issues and developments of interest to those responsible for protecting sensitive (unclassified) federal systems. Events are open to federal employees and their designated support contractors.

Topics of discussion at FCSM meetings in FY 2015 included briefings from various federal agencies on the Supply Chain, the Einstein 3 Accelerated (E3A) Reporting Tool, implementing privacy controls from Appendix J in SP 800-53, the U.S. Government Configuration Baseline (USGCB), the National Cybersecurity Center for Excellence (NCCoE), and SP 800-88 Revision 1, *Guidelines for Media Sanitation*.

This year's annual two-day offsite was held at NIST on August 26-27, 2015. Presentations included current technical, operational and management information systems security topics and updates on the information system security activities of OMB, GAO, the National Aeronautics and Space Administration (NASA), the National Archives and Records Administration (NARA), the Federal Aviation Administration (FAA), the U.S. Census Bureau, DHS, and NIST. Most presentations are available on the FCSM's website (see <http://csrc.nist.gov/groups/SMA/forum/>), under "Events."

- NIST Computer Security Division Update, Matthew Scholl, NIST;
- How to Best Protect Against Future Cyber Incidents, Trevor H. Rudolph, OMB;
- Implementing TIC E<sup>3</sup>A in Government and Using the XLA Threat Reduction and Correlation Tool (xTract™), Sandra Paul-Blanc, NARA, and Philip Kulp, XLA;
- GAO Information Security Update, Gregory C. Wilshusen, GAO;
- NIST SP 800-163, *Vetting the Security of Mobile Applications*, Steve Quirolgico, NIST;
- Using Risk Management to Improve Privacy in Information Systems, Ellen Nadeau, NIST;
- Framework for Improving Critical Infrastructure Cybersecurity, Matthew Barrett, NIST;
- Mobile Application Security and PIV Derived Credentials, Jane Maples, NASA and Peter Cauwels, NASA;
- Rethinking Cybersecurity from the Inside Out: An Engineering and Life Cycle-Based Approach for Building Trustworthy Resilient Systems, Ron Ross, NIST Fellow;
- How FAA Required 50,000+ People to Use PIV Cards in 2 Months, Myles Roberts, FAA;
- Cloud Assessments, John Connor, NIST;
- The National Vulnerability Database (NVD), Harold

Booth, NIST;

- Department of Transportation (DOT) Security Program Management Subcommittee's Information Assurance Policy Working Group (IAPWG), Kevin Sanchez-Cherry, DOT;
- Speak Out - Daniel Wood, Treasury – Term & Topic: PKI Landscape, Pat Toth, NIST – Request for topics for FY 2016 meetings;
- Information Technology (IT) Policy Initiatives Panel, Adam Sedgewick, NIST, William Fisher and Tim McBride, National Cybersecurity Center of Excellence (NCCoE); Mike Garcia, National Strategy for Trusted Identities in Cyberspace (NSTIC);
- U.S. Census Bureau Risk Management Program Implementation, Jaime Lynn Noble, U.S. Census Bureau; and
- DHS Continuous Diagnostics and Mitigation (CDM) Program Overview, Martin Stanley, DHS.

The Forum plays a valuable role in helping NIST and other federal agencies to develop and maintain a strong, proactive stance in the identification and resolution of new strategic and tactical IT security issues as they emerge. The number of members on the email list has grown steadily and provides a valuable resource for federal security program managers. To join, email your name, affiliation, phone number, title, and confirmation that you are a federal employee to [sec-forum@nist.gov](mailto:sec-forum@nist.gov); only .gov and .mil email addresses are accepted in the list serve.

#### For More Information, See:

<http://csrc.nist.gov/groups/SMA/forum/>

## CONTACTS:

Ms. Patricia Toth  
Chair  
(301) 975-5140  
[pthoth@nist.gov](mailto:pthoth@nist.gov)

Ms. Peggy Himes  
Administration  
(301) 975-2489  
[peggy.himes@nist.gov](mailto:peggy.himes@nist.gov)

## Federal Information Systems Security Educators' Association (FISSEA)

The Federal Information Systems Security Educators' Association (FISSEA), founded in 1987, is an organization hosted by NIST for information system security professionals to assist federal agencies in meeting their information system's security awareness, training, and education responsibilities. FISSEA strives to elevate the general level of information system security knowledge for the Federal Government and the federal workforce. It also seeks to assist the professional development of its members.



FISSEA membership is open to information system security professionals, professional trainers and educators, and managers responsible for information system security training programs in federal agencies, as well as contractors of these agencies and faculty members of accredited educational institutions who are involved in information security training and education. Willingness to share products, information, and experiences is all that is required to become a FISSEA member. A working group meets monthly to administer business activities.

FISSEA maintains a website, a mailing list, and participates in a social networking site as a means of communication for its members. CSD assists FISSEA with its operations by providing staff support for several of its activities and by being FISSEA's host agency.

The 28th Annual FISSEA Conference occurred March 24-25, 2015 at NIST. The FISSEA audience included managers responsible for information systems security awareness, training, certifications, workforce identification, compliance, etc. in federal agencies; contractors providing awareness and training support; and faculty members of accredited educational institutions who are involved in information security training and education. Pat Toth, Peggy Himes, and Judy Barnard (NIST), as well as Gretchen Morris (DB Consulting/NASA), and other members of the FISSEA Working Group, were integral to the effort to support the conference.

This year's theme was "Changes, Challenges, and Collaborations: Effective Cybersecurity Training". Attendees gained new techniques for developing/conducting training, cost-effective practices, workforce development, and free resources and contacts. Over 200 cybersecurity training professionals attended the two-day conference.

NIST's Information Technology Laboratory (ITL) Director, Charles Romine, welcomed attendees to the event. We were honored to have Dr. Neil Grunberg, Professor of Military and Emergency Medicine, Uniformed Services University, who provided an inspiring keynote presentation, "Information Security System Educators Must be Leaders." His talk addressed the leadership and communication skills needed by Cybersecurity Educators

Presenters represented NIST, DHS, the Department of State (DoS), the National Security Agency (NSA), private industry, and academia. Attendees had an opportunity to visit 16 vendors and federal agencies on the second day to share and tell about their specific awareness and training programs.



**Figure 6: Pecha-Kucha Participants (left to right): Art Chantker, Potomac Forum, Frank Cicio Jr, iQ4 Corporation, Sandy Toner, ICF International, and Louis Numkin, FISSEA Life Member**

FISSEA conferences include Pecha Kucha (Lightning Rounds) sessions. Speakers have 6 minutes 40 seconds for their presentations, and the challenge is in limiting one's talk to only 20 slides. It's challenging to do as a speaker and quite fun for the audience to watch, so the Pecha Kucha fast-paced talks proved to be entertaining and educational.

The FISSEA Educator of the Year Award was established to recognize and honor a contemporary who is making special efforts to create, build, manage, or inspire an information systems security awareness, training, or education program. Sam Maroon presented the FISSEA 2014 Educator of the Year posthumously to Shon Harris of Logical Security. Mr. Maroon shared Ms. Harris' contributions to the cybersecurity education industry by characterizing her contributions in three ways: as a writer, a trainer, and a thought leader. Ms. Harris' friends and colleagues, Michael Lester and Hamid Dehghan accepted the plaque on her behalf.



**Figure 7: Friends and colleagues accepting the FISSEA Educator of the Year on behalf of Ms. Harris**

Other traditional FISSEA conference events include announcing the winners of the FISSEA security contest. The FISSEA Security Awareness, Training & Education Contest includes five categories from one of FISSEA's three key areas of Awareness, Training, and Education. A winner is selected from each category and awarded a certificate. The categories include: (1) an awareness poster; (2) motivational item (e.g., trinkets, pens, stress relief items and t-shirts); (3) an awareness website; (4) an awareness newsletter; and (5) role-based training & education.

### 2015 FISSEA Awareness, Training, and Education Contest Winners

Awarded Certificates at the Conference (selected by an impartial judging committee prior to the conference):

**Poster Winner:** Kelly Wright – Veteran Affairs (VA) IT Workforce Development;

**Website Winner:** NASA IT Security Awareness and Training Center Team;

**Motivational Item Winner:** Jane Moser – Employment and Social Development Canada (ESDC);

**Newsletter Winner:** Wendy Andrews, Robert Collins, Arnold Ginn, and CDR Steven Miller – Indian Health Service; and

**Role-Based Training Winner:** Jane Moser –ESDC.

Peer's Choice Awards (selected by peers during the conference):

**Poster Winner:** Kimberly Conway, Sara Fitzgerald, Sean Hanion, Dave Stapleton, and Steven VanBrackle, FDA;

**Website Winner:** Kimberly Conway, Sara Fitzgerald, Sean Hanion, Dave Stapleton, and Steven VanBrackle, FDA;

**Motivational Item Winner:** Cindy Dailey, Geisinger Health System;

**Newsletter Winner:** Brenda L. Ellis, NASA; and

**Role-Based Training Winner:** Jennifer Young, Communication Security Establishment.

Another bonus of attending the 2015 FISSEA conference was networking. The conference continues to be a valuable forum for individuals from government, industry, and academia who are involved with information systems/ cybersecurity workforce development. Attendees gain insights regarding information security awareness, training, education, certification, and professionalization. Attendees also learn of ongoing and planned training and education programs and cybersecurity initiatives. It provides NIST the opportunity to provide assistance to departments and agencies as they work to meet their FISMA responsibilities. The FISSEA website provides links to the Conference Program, and also links to presentations (<http://csrc.nist.gov/fissea>).

The next conference will be held at NIST on March 15-16, 2016.

### For More Information, See:

<http://csrc.nist.gov/fissea>

## CONTACTS:

Ms. Patricia Toth  
(301) 975-5140

[patricia.toth@nist.gov](mailto:patricia.toth@nist.gov)

Ms. Peggy Himes  
(301) 975-2489

[peggy.himes@nist.gov](mailto:peggy.himes@nist.gov)

## Information Security and Privacy Advisory Board (ISPAB)

Since the inception of this Advisory Board in 1987, the Information Security and Privacy Advisory Board (ISPAB) has successfully renewed its charter with proper authority every two years. The Board plays a central and unique role in providing the government with expert advice concerning information security and privacy issues that may affect federal information systems. Title III of the E-Government Act of 2002 reaffirmed the need for this Board by giving it an additional responsibility: to thoroughly review all of the proposed information technology standards and guidelines developed under Section 20 of the National Institute of Standards and Technology Act (15 U.S. Code (U.S.C.) 278g-3), as amended.

The ISPAB is a federal advisory committee with specific statutory objectives to identify emerging managerial,

technical, administrative, and physical safeguard issues related to information security and privacy. The Board was originally created by the Computer Security Act of 1987 (P.L. 100-235) as the Computer System Security and Privacy Advisory Board (CSSPAB) within the Department of Commerce. The CSSPAB was chartered in May 1988 in accordance with the Federal Advisory Committee Act, as amended. The 2002 FISMA legislation amended the statutory authority of the Board and provided its current name.

The duties of the Board, as stipulated in FISMA, include:

- Identification of emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy;
- Advising NIST and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems (including the thorough review of proposed standards and guidelines developed under 15 U.S.C. 278g-3 - Computer Standards Program); and
- Annually reporting its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of NSA, and the appropriate committees of Congress.

Congress indicated the long-term need for the Board by setting the term of Board members to four years. The charter requires that the NIST Director appoint the Chairperson and all twelve members of the Board. They are selected for their preeminence in the information technology industry or related disciplines.

The 15 U.S.C. 278g-4 charter stipulates that Board members be selected from three main categories, with each category providing four members. Category 1 includes members from outside the Federal Government who are eminent in the information technology industry, at least one of whom is a representative of small or medium-sized companies in such industries. Category 2 also includes members from outside the Federal Government who are eminent in the field of information technology or related disciplines, but who are not employed by or representative of a producer of information. Category 3 includes those from the Federal Government who are experienced in information system management, including those with experience in information security and privacy, at least one of whom should be from the National Security Agency. The categorization of Board members is intended to meet ISPAB's statutory objectives. Federal members bring a detailed understanding of the federal processing environment; industry brings concerns and experiences regarding product development and market formation, while private computer security experts are able to bring their experiences of commercial cost-effective security measures into Board discussion.

Dr. Peter Weinberger is currently the Chair of ISPAB. Dr. Weinberger, a Computer Scientist from Google, joined the Board in 2008 and assumed the responsibilities of the Chair in January 2015. He is also a Co-Chair of a National Academies study on fundamental work in cybersecurity, and a member of the National Academies study on Presidential Policy Directive (PPD) 28, *Signals Intelligence Activities*. He is well supported by the following Board members (see <http://csrc.nist.gov/groups/SMA/ispab/membership.html>):



**Figure 8: From Left to Right – Annie Sokol (Designated Federal Officer, CSD, NIST), Greg Garcia, Ed Roback, Toby Levin, Jeffrey Greene, John Centafont, Dr. Kevin Fu, Dr. Peter Weinberger (Chair, ISPAB), Matt Scholl (Chief, CSD, NIST)**  
**Members not included in this picture: Chris Boyer, Dr. Ana Anton, David Cullinane, Gale Stone, and J. Daniel Toler**



- Ana (Annie) Antón, Professor and Chair, School of Interactive Computing, Georgia Institute of Technology;
- Christopher Boyer, Assistant Vice President, Public Policy, AT&T;
- John R. Centafont, NSA Information Assurance and Cyber Defense;
- David Cullinane, CEO, TruStar, LLC;
- Dr. Kevin Fu, Associate Professor, The University of Michigan;
- Gregory Garcia, Executive Vice President, McBee Strategic;
- Jeffrey Greene, Esq., Director, Government Affairs, North America & Senior Policy Counsel, Senior Policy Counsel, Cybersecurity and Identity, Symantec Corporation;
- Toby Levin, Retired (formerly Senior Advisor and Director of Privacy Policy, U.S. DHS);
- Edward Roback, Associate Chief Information Officer for Cyber Security, U.S. Department of Treasury; and
- Gale Stone, Deputy Assistant Inspector General for Audit, Social Security Administration (SSA).

During FY 2014-2015, ISPAB held three meetings, all in Washington D.C:

- October 22-24, 2014;
- February 11-13, 2015; and
- June 10-12, 2015.

In keeping with previous practices at the first meeting of each fiscal year, the Board established a work plan for FY 2015 at the meeting in October 2014. The resulting plan included the following areas of focus:

- Cryptography, and specifically NIST R&D;
- Federally funded Research and Development Centers (FFRDCs) – internally, externally and control balance;
- Metrics – success measure for security and privacy;
- Trust in NIST (accountability and success);
- Quantum mechanics;
- Identity management (Biometrics);
- Privacy technology – implementation methodology;
- Medical devices – security, privacy and safety, Health-care IT Security;

- FISMA – Continuous Diagnostics and Mitigation (CDM) and Federal Risk and Authorization Management Program (FedRAMP);
- CDM – Communications Security, Reliability and Interoperability Council (CSRIC), Trusted Internet Connection (TIC);
- Key ESCROW – history and lessons learned
- Cybersecurity; and
- Updates of other critical NIST publications.

In aligning with the work-plan focus areas, the Board expanded its work to include the following:

- The Privacy and Civil Liberties Oversight Board (PCLOB);
- OMB Circular A130 Revised;
- Acquisition, Supply Chain Security, and Open Source trustworthy software;
- Mobile Devices and the Protection of Sensitive Information;
- Intelligence and communication technologies;
- Cryptography and NIST Cryptographic standards processes;
- The NIST Cybersecurity Framework;
- Safeguarding Health Information;
- The Controlled Unclassified Information (CUI) Program;
- Breach and breach reporting;
- The Federal Information Security Management Act (FISMA);
- Emerging Technologies: Cloud Computing, Big Data, the Internet of Things, Cyber Physical Systems, Smart cities, Drones and Unmanned Aircraft Systems, Medical Devices, Transportation Sector and Vehicle-to-Vehicle Communication, and relating impacts on security and privacy;
- The National Strategy for Trusted Identities in Cyberspace (NSTIC);
- The National Cybersecurity Center of Excellence (NC-CoE); and
- The realignment of the Information Technology Laboratory.

The presenters at each Board meeting were leaders and experts representing private industry, academia, federal agency Chief Information Officers (CIOs), Inspector Generals (IGs) and Chief Information Security Officers (CISOs).

Copies of the current list of members and their biographies, the Board's charter and past Board activities are located at <http://csrc.nist.gov/groups/SMA/ispab>. Information on ISPAB Meetings is published in Federal Register Notices at least 16 days prior to the meeting. Those interested in receiving meeting notices and other notices relating to NIST work in information security and privacy may email their name, affiliation, and address to Annie Sokol at the address below.

**For More Information, See:**

<http://csrc.nist.gov/groups/SMA/ispab>

---

**CONTACT:**

Ms. Annie Sokol  
Designated Federal Officer (DFO), ISPAB  
(301) 975-2006  
[annie.sokol@nist.gov](mailto:annie.sokol@nist.gov)

**Small and Medium Size Business (SMB)  
Cybersecurity Workshop Outreach**

Small business owners face a broad range of information security issues. A computer failure or system breach could jeopardize the company's reputation and may result in significant damage and recovery cost, or going out of business. The small business owner who recognizes the threat of computer crime and takes steps to deter inappropriate activities is less likely to become a victim.

The U.S. Small Business Administration (SBA) reports that over 27 million U.S. companies - more than 99 percent of all U.S. businesses - are SMBs of 500 employees or fewer (see <http://www.sba.gov/sites/default/files/allprofiles12.pdf>). While the threats to individual SMBs may not be significantly different from those facing larger organizations, an SMB frequently has fewer resources available to protect systems, detect attacks, or respond to security issues. A vulnerability common to a large percentage of SMBs could pose a threat to the nation's information infrastructure and economic base.

To help address information security risk, these businesses require assistance with the identification of security mechanisms and with practical, cost-effective training. Training helps SMB's use their limited resources most effectively to address relevant and serious threats. In response to this need, NIST, the SBA, and the Federal Bureau of Investigation (FBI) InfraGard program co-sponsor a series of cybersecurity training workshops for small businesses. These workshops provide an overview of cybersecurity

threats, vulnerabilities, and corresponding protective tools and techniques, with a special emphasis on information that small business personnel can apply directly.

In FY 2015, six SMB outreach workshops were provided in Reno, Nevada; Fresno, California; Modesto, California; Fairmont, West Virginia; Pittsburgh, Pennsylvania; and McHenry, Maryland. Additionally, the SMB Cybersecurity Outreach Program was briefed to the InfraGard National Congress.

In collaboration with the SBA and the FBI, planning is underway to identify locations and plan cybersecurity workshops in FY 2016.

**For More Information, See:**

<http://csrc.nist.gov/groups/SMA/sbc/>

---

**CONTACT:**

Ms. Patricia Toth  
301-975-5140  
[patricia.toth@nist.gov](mailto:patricia.toth@nist.gov)

## CRYPTOGRAPHIC STANDARDS PROGRAM

### Hash Algorithms and the Secure Hash Algorithm-3 (SHA-3) Standard (FIPS 202)

NIST opened a public competition in 2007 to develop a new cryptographic hash algorithm, SHA-3, to augment the hash algorithms specified in FIPS 180-4, *Secure Hash Standard (SHS)*. The competition ended on October 2, 2012 when NIST announced the selection of **KECCAK** as the winning algorithm for standardization as the new SHA-3 Standard. NIST consulted with the **KECCAK** designers and the cryptographic community, and developed a SHA-3 standardization plan that was presented at numerous cryptography conferences and posted at the NIST hash website, indicated below, for public feedback.

NIST announced Draft FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, in the Federal Register (79 FR 30549) on May 28, 2014 and requested comments (see <https://federalregister.gov/a/2014-12336>). The announcement also proposed a revision of the Applicability Clause of the Announcement Section of FIPS 180-4, *Secure Hash Standard*, to allow the use of hash functions specified in either FIPS 180-4 or FIPS 202, modifying the original mandate to use only the hash functions specified in FIPS 180-4. The other sections of FIPS 180-4 remain unchanged. A ninety-day public comment period was provided, which ended on August 26, 2014.

NIST received seven comments on Draft FIPS 202 and one comment on the Draft Revision of the Applicability Clause of FIPS 180-4. All comments received are posted at the NIST hash website. None of the comments opposed the adoption of the SHA-3 Standard or the revision of the Applicability Clause of FIPS 180-4. NIST also received public feedback at the 2014 SHA-3 Workshop and afterwards. All of the comments were carefully reviewed, and changes were made to FIPS 202, where appropriate. NIST made additional editorial changes to improve FIPS 202.

FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, and the revised Applicability Clause of FIPS 180-4 were approved by the Secretary of Commerce and announced in the Federal Register (80 FR 46543) on August 5, 2015 (see <https://federalregister.gov/a/2015-19181>). FIPS 202 and FIPS 180-4 are available at: <http://csrc.nist.gov/publications/PubsFIPS.html>.

#### For More Information, See:

[http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3\\_standardization.html](http://csrc.nist.gov/groups/ST/hash/sha-3/sha-3_standardization.html)

36

## CONTACT:

Ms. Shu-jen Chang  
(301) 975-2940  
[shu-jen.chang@nist.gov](mailto:shu-jen.chang@nist.gov)

### Random Number Generation (RNG)

Random numbers are required for the security for many cryptographic algorithms. For example, random numbers are used to generate the keys needed for encryption and digital signature applications.

In March 2007, CSD published SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, which contained four deterministic random bit generator (DRBG) mechanisms, two based on hash functions, one based on the use of block cipher algorithms and one based on the use of elliptic curves. This recommendation was revised as SP 800-90A in January 2012 to include additional capabilities and in June 2015 to remove the DRBG based on the use of elliptic curves, i.e., the DUAL\_EC\_DRBG, since its security has been in question.

Two additional documents (SP 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation*, and SP 800-90C, *Recommendation for Random Bit Generator (RBG) Constructions*) are under development, and the initial drafts were made available for public comment in 2012.

SP 800-90B addresses the development and testing of entropy sources, including descriptions of the tests for NIST's Cryptographic Algorithm Validation Program to validate candidate entropy sources. An entropy source depends on a noise source, which is the root of security for the entropy source. During FY 2015, the CTG developed and tested additional methods for estimating the amount of entropy per noise-source output. An overview of the methodology and preliminary results of new estimators, called predictors, were presented at ShmooCon in the talk "How Random is Your RNG?" Further details and results were published in the paper "Predictive Models for Min-Entropy Estimation" at the *Cryptographic Hardware and Embedded Systems (CHES 2015)* workshop. A new draft of SP 800-90B will be provided for another public comment period in early FY 2016.

SP 800-90C provides basic guidance on the construction of RBGs from the entropy sources validated against the requirements of SP 800-90B and the DRBG mechanisms of SP 800-90A. The CTG plans to provide a new version of this document for public comment prior to the end of the SP 800-90B public-comment period.



A public workshop is planned for FY 2016 to discuss SP 800-90B and 90C.

**For More Information, See:**

<http://csrc.nist.gov/groups/ST/toolkit/rng/>

## CONTACTS:

Ms. Elaine Barker  
(301) 975-2911  
[elaine.barker@nist.gov](mailto:elaine.barker@nist.gov)

Mr. John Kelsey  
(301) 975-5101  
[john.kelsey@nist.gov](mailto:john.kelsey@nist.gov)

Dr. Meltem Sönmez Turan  
(301) 975-4391  
[meltem.turan@nist.gov](mailto:meltem.turan@nist.gov)

Dr. Kerry McKay  
(301) 975-4969  
[kerry.mckay@nist.gov](mailto:kerry.mckay@nist.gov)

## Block Cipher Modes of Operation

The engine for many of the techniques in NIST's cryptographic toolkit is a block cipher algorithm, such as the Advanced Encryption Standard (AES) algorithm or the Triple Data Encryption Algorithm (TDEA). A block cipher transforms some fixed-length binary data (i.e., a "block") into seemingly random data of the same length. The transformation is determined by the choice of some secret data called the "key." The same key is used to reverse the transformation and recover the original block of data. A cryptographic technique that is constructed from a block cipher is called a mode of operation. Several modes of operation have been specified in the SP 800-38 series of publications.

The CTG has nearly completed the development of two AES modes of operation for format-preserving encryption (FPE), based on proposals that were submitted from the private sector. A format can be a sequence of decimal digits, such as a credit card number or a social security number; formats can also be defined for other sets of characters besides decimal digits. FPE is expected to facilitate the retrofitting of encryption to existing applications. For example, FPE could be applied to database systems, so that sensitive data could be targeted for encryption without disrupting the underlying data fields/pathways.

The two modes of operation for FPE, called FF1 and FF3, will be specified in Special Publication 800-38G, *Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption*, which will be completed in FY 2016.

In the coming year, the CTG plans to consider technical changes to two other Special Publications in the 800-38 series. In particular, the CTG plans: 1) to solicit public comment on requirements for the generation of non-repeating IVs for the Galois/Counter Mode, specified in SP 800-38D,

*Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*; and 2) to revisit the combinations of encryption and authentication that are approved in SP 800-38F, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*.

**For More Information, See:**

<http://csrc.nist.gov/groups/ST/toolkit/BCM/>

## CONTACT:

Dr. Morris Dworkin  
(301) 975-2354  
[morris.dworkin@nist.gov](mailto:morris.dworkin@nist.gov)

## Key Management

Key management is required for applying numerous cryptographic technologies and is considered the most critical aspect associated with the use of cryptography. CSD began to provide guidance in managing the keys used for cryptographic applications in the late 1990s to early 2000s. Several guidance and recommendation documents have been and continue to be developed in the form of NIST Special Publications (SP), which have been periodically updated to address new algorithms and handling procedures. These documents are coordinated with federal agencies and with the cryptographic community, including national and international organizations, industry, and academia. During FY 2015, the following publications were either created or revised.

SP 800-57, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance*, was first published in 2009. This document addresses the key-management issues of currently available cryptographic mechanisms, including the use of Public Key Infrastructures (PKI) and several commonly used security protocols and applications. A revision of this document was provided for public comment in May 2014 that updated the guidance provided in the 2009 version, included an additional section on the Secure Shell (SSH) protocol, and substituted a reference to SP 800-52, Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, for the TLS section. After the comment period, the draft revision was revised, and published in January 2015.

SP 800-57, *Recommendation for Key Management, Part 1: General*, was first published in 2005, and later revised in 2007 and 2012. Another revision was provided for public comment in FY 2015 that includes information on and references to recent work performed by CSD; removed references to the Dual\_EC\_DRBG, which was removed

from SP 800-90A, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, revised the security-strength tables; and revised the key-state discussion to provide more clarification. The revision was provided for public comment in September 2015 and should be completed in early FY 2016.

SP 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, was originally published in January 2011. This document provides specific guidance for transitions to the use of stronger cryptographic keys and more robust algorithms. An update of SP 800-131A was provided for public comment and completed in November 2015. This update removes approval for the Dual\_EC\_DRBG, deprecates the use of non-approved key-establishment schemes, disallows the use of non-approved key-wrapping methods after 2017, and indicates that the use of the SHA-3 family of hash functions as acceptable.

SP 800-152, *A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)*, provides guidance on the CKMSs to be used by the Federal Government. This document provides refinements of the requirements for CKMS designers that are specified in SP 800-130, *A Framework for Designing Cryptographic Key Management Systems*. SP 800-152 also provides requirements and recommendations for the service providers of CKMSs used by federal agencies and their contractors, as well as guidance for the federal agencies in selecting a CKMS that supports the security and management policies of those agencies. A draft of this document was provided for public comment in FY 2013, and a workshop was held in March 2013 to discuss the draft. A second draft was provided for comment in FY 2015, and a final version addressing the received comments was published in October 2015.

A new NIST publication is under development that provides guidance on the security strength of a cryptographic key that is used to protect data (i.e., a data-protection key), given the manner in which the key was generated and handled. This document, SP 800-158, *Key Management: Obtaining a Targeted Security Strength*, involves a considerable amount of new research, since it is an area that has not been fully addressed to date. This publication will be available for public comment in FY 2016.

Additional key-management work to be conducted in FY 2016 includes revision(s) to SP 800-56A, *Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography*, and SP 800-56B, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*, to allow the use of larger key sizes.

## For More Information, See:

[http://csrc.nist.gov/groups/ST/key\\_mgmt](http://csrc.nist.gov/groups/ST/key_mgmt)

## CONTACTS:

Ms. Elaine Barker  
(301) 975-2911  
[elaine.barker@nist.gov](mailto:elaine.barker@nist.gov)

Dr. Lily Chen  
(301) 975-6974  
[lily.chen@nist.gov](mailto:lily.chen@nist.gov)

Mr. Quynh Dang  
(301) 975-3610  
[quynh.dang@nist.gov](mailto:quynh.dang@nist.gov)

Dr. Dustin Moody  
(301) 975-8136  
[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)

Mr. Ray Perlner  
(301) 975-3357  
[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)

## Transport Layer Security

SP 800-52, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, provides recommendations regarding TLS server and client implementations. TLS is a widely used cryptographic protocol that provides communication security for a variety of network applications, such as email, e-commerce, and healthcare.

SP 800-52 was first published in 2005, and SP 800-52 Revision 1 was published in April 2014. Since the revision, CTG has been following developments in TLS implementations, including updates and attacks. In FY 2016, a second revision will be published that considers these developments. This second revision will be a minor update to SP 800-52 Revision 1.

The Internet Engineering Task Force (IETF) is actively developing extensions that can be used to add functionality to TLS. CSD will continue to review updates and additions to the TLS protocol in FY 2016.

## CONTACTS:

Dr. Lily Chen  
(301) 975-6974  
[lily.chen@nist.gov](mailto:lily.chen@nist.gov)

Dr. Kerry McKay  
(301) 975-4969  
[kerry.mckay@nist.gov](mailto:kerry.mckay@nist.gov)

## Elliptic Curve Cryptography

Elliptic curve cryptography is critical to the adoption of strong cryptography as we migrate to higher security strengths. NIST has standardized elliptic curve cryptography for digital signature algorithms in FIPS 186 and for key establishment schemes in SP 800-56A.

In FIPS 186-4, NIST recommends fifteen elliptic curves of varying security levels for use in these elliptic curve cryptographic standards. However, the provenance of the curves is not fully specified in the standard, leading to recent public concerns that there could be a hidden weakness in these curves. NIST is not aware of any vulnerability in these curves when they are implemented correctly and used as described in NIST standards and guidelines.

However, more than fifteen years have passed since these curves were developed, and the community now knows more about the security of elliptic curve cryptography and practical implementation issues. Advances within the cryptographic community have led to the development of new elliptic curves and algorithms whose designers claim to offer better performance and are easier to implement in a secure manner. Some of these curves are under consideration in voluntary, consensus-based Standards Developing Organizations.

In June 2015, NIST hosted a workshop on Elliptic Curve Cryptography Standards to discuss possible approaches to promote the adoption of secure, interoperable and efficient elliptic curve mechanisms. Workshop participants expressed significant interest in the development, standardization and adoption of new elliptic curves. As a result of this input, NIST is considering the addition of new elliptic curves to the current set of recommended curves in FIPS 186-4. In FY 2016, NIST will solicit comments on possible improvements to FIPS 186-4, which may lead to a workshop held later in the year.

## CONTACTS:

Email project team: [EllipticCurves@nist.gov](mailto:EllipticCurves@nist.gov)

Dr. Dustin Moody  
(301) 975-8136

[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)

Dr. Lily Chen

(301) 975-6974

[lily.chen@nist.gov](mailto:lily.chen@nist.gov)

Mr. Andy Regenscheid

(301) 975-5155

[andy.regenscheid@nist.gov](mailto:andy.regenscheid@nist.gov)

## Post-Quantum Cryptography

In recent years, there has been a substantial amount of research on quantum computers – machines that exploit quantum mechanical phenomena to solve problems that are difficult or intractable for conventional computers. If large-scale quantum computers are ever built, they will be able to break the existing infrastructure of public-key cryptography. The focus of the Post-Quantum Cryptography project is to identify candidate quantum-resistant systems that are

secure against both quantum and classical computers, as well as the impact that such post-quantum algorithms will have on current protocols and security infrastructures.

In FY 2015, NIST researchers held regular seminars. The presentation topics included the latest published results; a synopsis of the security analysis; and status reports in the areas of quantum computation, hash-based signatures, coding-based cryptography, lattice-based cryptography, and multivariate cryptography. Through these presentations and discussions, the team made significant progress in understanding the strengths and weaknesses of the existing cryptographic schemes in each category. The project team is planning to create evaluation criteria for post-quantum cryptography schemes for standardization.

The NIST team continues to be productive in post-quantum cryptography research. The results have been published at the major conferences, such as PQCrypto 2014, and Eurocrypt 2015. NIST researchers have given presentations at conferences and workshops to increase awareness of the upcoming migration. NIST researchers have contributed to the European Telecommunications Standards Institute (ETSI) whitepaper on quantum-safe cryptography. NIST has also sponsored other research, education, and research events.

NIST held the *Workshop on Cybersecurity in a Post-Quantum World* in March of 2015. The workshop was attended by approximately 140 participants from around the world. Presentations given at the workshop included new proposals for quantum-safe cryptosystems, ideas for how to modify protocols (such as TLS) to include these new cryptosystems, discussions on how to standardize hash-based signatures and key-management issues, as well as new ideas on the cryptanalysis of the many post-quantum systems.

In FY 2016, NIST will continue to explore the security and feasibility of purported quantum-resistant technologies, with the ultimate goal of uncovering the fundamental mechanisms necessary for efficient, trustworthy, and cost-effective information assurance in the post-quantum era. Upon the successful completion of this phase of the project, NIST will be prepared for possible standardization efforts in this area.

### For More Information, See:

<http://csrc.nist.gov/groups/ST/post-quantum-crypto/>



## CONTACTS:

Email project team: [pqc@nist.gov](mailto:pqc@nist.gov)

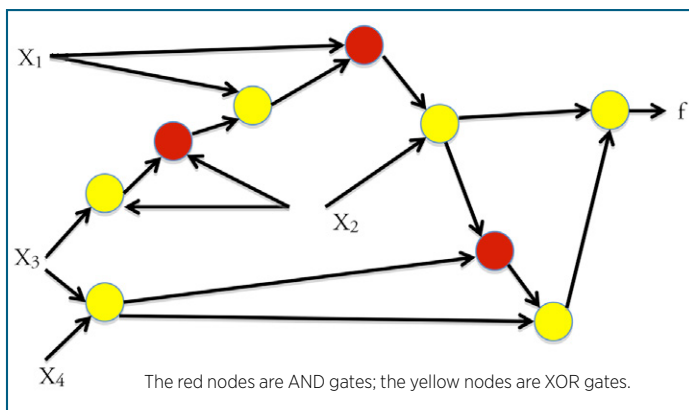
Dr. Dustin Moody  
(301) 975-8136  
[dustin.moody@nist.gov](mailto:dustin.moody@nist.gov)

Dr. Lily Chen  
(301) 975-6974  
[lily.chen@nist.gov](mailto:lily.chen@nist.gov)

Dr. Yi-Kai Liu  
(301) 975-6499  
[yi-kai.liu@nist.gov](mailto:yi-kai.liu@nist.gov)

## Circuit Complexity

Cryptographic functions, such as encryption, digital signatures, and hashing, are implemented as electronic circuits for a wide class of applications. In practice, it is important to be able to minimize the size of these circuits. This problem is closely related to designing small combinational circuits. These circuits use only binary AND, XOR and NEGATION gates, i.e., multiplication, addition, and “+1” in arithmetic modulo 2. A combinational circuit on four variables ( $X_1$ ,  $X_2$ ,  $X_3$ , and  $X_4$ ) using AND and XOR gates is depicted in Figure 9.



**Figure 9: Combinational Boolean Circuit**

The project team has shown that finding optimal combinational circuits is MAX-SNP Complete. In practice, this means that it is necessary to settle for methods that design “good” circuits, as opposed to provably optimal circuits. The CTG has developed and implemented new solutions for the circuit-minimization problem. Two patents have been granted related to this work, the last one in FY 2014. These are held jointly between NIST and the University of Southern Denmark.

The CTG is also researching circuit-based security metrics for cryptographic functions. For a function to be secure (in particular, one-way), it must be the case that any circuit that implements it is sufficiently complex. In particular,

40

a function is insecure if it can be implemented by a circuit containing too few Boolean AND gates. This security metric, namely the number of AND gates necessary and sufficient to implement a function, is referred to as its multiplicative complexity. Unfortunately, determining multiplicative complexity is extremely hard (very recently, Magnus Find proved computational intractability conditioned on the existence of one-way functions). Mathematicians attempted to determine multiplicative complexity in the 1970s, but the effort had been largely abandoned by the 1980s. However, the CTG has published circuits that are provably optimal or close to optimal (with respect to multiplicative complexity) for important classes of functions. In the process, we developed tools that have wide applicability for both theoretical and applied research in security and cryptography.

Multiparty computation is a technique that allows a group of people to compute a function of their inputs without revealing the inputs themselves. Examples of this are: i) holding an election; ii) conducting closed-bid auctions in which only the winning bid is determined; iii) proving to a third party that a person’s encrypted attributes satisfy some requirement, such as “over 21 and (U.S. citizen or Canadian citizen)”. The protocols that solve multiparty computation problems often encrypt bits using arithmetic modulo 2. The complexity of such protocols largely depends on the number of multiplications required. Hence, expressing functions as circuit computations with only a few multiplication (AND) gates is important. Some of the published circuits are now the standard reference for benchmarking tools in multiparty computation.

The following is a partial list of new results by our team:

- The smallest known circuits were constructed for multiplication in several small finite fields.
- The smallest known circuits were constructed for binary multiplication (i.e., multiplication of polynomials of degree  $n$  over the Galois Field with two elements). This yields important speed increases in elliptic curve cryptography.
- Optimal circuits were constructed - with respect to multiplicative complexity - for all predicates on four bits (see the example below). There are 65,536 such predicates. Surprisingly, the multiplicative complexity of all these functions turned out to be at most three. Additionally, our circuits use no more than seven non-linear gates (XOR, XNOR). This is quite hard. Consider the following predicate (arithmetic is modulo 2):  
$$f = x_1 + x_2 + x_3 + x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_3x_4.$$
Computing the last term requires three multiplications. So, it is quite surprising that the full expression can be

computed using only three multiplications. But, we have shown this to be true for  $\mathcal{F}$  and all other predicates on four bits. The circuit on the previous page computes  $\mathcal{F}$  using three multiplications and six additions.

- A proof was developed that the maximum multiplicative complexity of predicates on five bits (there are more than 4 billion such predicates) is four. The proof is constructive, meaning that the circuits can actually be built.
- A proof was developed that an explicit function requires at least  $3.01n$  gates. This constitutes the only improvement on this problem for more than 30 years. The result is due to Magnus Find, in collaboration with mathematicians from New York University (NYU) and from the Steklov Institute, St. Petersburg, Russia.

Circuits are posted periodically at <http://www.cs.yale.edu/homes/~peralta/CircuitStuff/CMT.html>

## CONTACT:

Dr. René Peralta  
(301) 975-8702  
[rene.peralta@nist.gov](mailto:rene.peralta@nist.gov)

## Cryptography for Constrained Environments

There are several emerging areas in which highly constrained devices are interconnected, typically communicating wirelessly with one another, and working in concert to accomplish some task. Examples of these areas include: sensor networks, distributed control systems, the Internet of Things, cyber physical systems, and the smart grid. Security and privacy can be very important in all of these areas. Because the majority of current cryptographic algorithms were designed for desktop/server environments, implementing many of these algorithms with constrained resources can be extremely challenging. If current algorithms can be made to fit into the limited resources of constrained environments, their performance is typically not acceptable.

CTG staff are examining applications in constrained environments to determine whether NIST should develop lightweight cryptographic standards. CTG is communicating with industry experts to understand challenges, limitations and work from other standardization bodies in this area. In FY 2015, CTG organized a NIST workshop on *Lightweight Cryptography* in Gaithersburg, MD, July 20-21, 2015 to discuss issues related to the security and resource requirements of applications in constrained environments

and potential future standardization of lightweight primitive algorithms. The workshop included two invited talks, twenty-four presentations and a panel discussion.

In FY 2015, CTG staff further engaged the international cryptographic community by providing presentations at the *Fourth International Workshop on Lightweight Cryptography for Security and Privacy* in Bochum, Germany, at the *Fast Software Encryption Workshop* in Istanbul, Turkey and at the *Lightweight Crypto Day*, in Haifa Israel. Project summaries and challenges ahead were presented at the Cybersecurity Innovation Forum and to ITL's Cyber-Physical Systems (CPS) group.

In FY 2016, CTG will continue to analyze the resource requirements and performance characteristics of lightweight primitives, and study their use as building blocks to perform various cryptographic objectives. Additionally, CTG is planning to publish a report that describes the current state and challenges in target application areas.

## CONTACTS:

Mr. Lawrence Bassham  
(301) 975-3292  
[lawrence.bassham@nist.gov](mailto:lawrence.bassham@nist.gov)

Dr. Kerry McKay  
(301) 975-4969  
[kerry.mckay@nist.gov](mailto:kerry.mckay@nist.gov)

Dr. Meltem Sönmez Turan  
(301) 975-4391  
[meltem.turan@nist.gov](mailto:meltem.turan@nist.gov)

## The NIST Randomness Beacon

NIST has implemented a source of public randomness. The service is available at <https://beacon.nist.gov/home>. It uses two independent, commercially available sources of randomness, each with an independent hardware entropy source and SP 800-90A-approved components.

The NIST Beacon is designed to provide *unpredictability*, *autonomy*, and *consistency*. *Unpredictability* means that users cannot algorithmically predict bits before they are made available by the source. *Autonomy* means that the source is resistant to attempts by outside parties to alter the distribution of the random bits. *Consistency* means that a set of users can access the source in such a way that they are confident of receiving the same random string.

The NIST Beacon posts bit-strings in blocks of 512 bits every 60 seconds. Each such value is time-stamped and signed, and includes the hash of the previous value to chain the sequence of values together. This prevents all parties, even the source, from retroactively changing an output packet without being detected. The NIST Beacon keeps

all output packets. At any point in time, the full history of outputs is available to users.

Tables of random numbers have probably been used for multiple purposes at least since the Industrial Revolution. In the digital age, algorithmic pseudorandom number generators (PRNGs) have largely replaced these tables. The NIST Beacon expands the use of randomness to multiple scenarios in which neither tables nor PRNGs can be used. The extra functionalities stem mainly from three features. First, the Beacon-generated numbers cannot be predicted before they are published. Second, the public, time-bound, and authenticated nature of the Beacon allows a user application to prove to anybody that it used truly random numbers not known before a certain point in time. Third, this proof can be presented offline and at any point in the future.

Although commercially available physical sources of randomness are adequate as entropy sources for currently envisioned implementations of the NIST Beacon, we are working on developing a source of *verifiably random* sequences. In collaboration with NIST physicists from the Physical Measurement Laboratory (PML), we aim to use quantum non-locality to build an entropy source whose unpredictability is guaranteed by the laws of physics. This project is funded by NIST's Innovations in Measurement Science (IMS) Program. IMS funds highly competitive projects designed to explore high-risk, leading-edge research concepts that anticipate the future measurement and standards needs of industry and science. For more information on this collaboration see [http://www.nist.gov/pml/div684/random\\_numbers\\_bell\\_test.cfm](http://www.nist.gov/pml/div684/random_numbers_bell_test.cfm).

As of the end of FY 2015, the NIST Beacon has been functioning without interruption for more than two years. NIST encourages the community at large to research and publish novel ways in which this tool can be used. A few examples of applications are *unpredictable sampling*, *new authentication mechanisms*, and *secure multi-party computation*.

**For More Information, See:**

[http://www.nist.gov/itl/csd/ct/nist\\_beacon.cfm](http://www.nist.gov/itl/csd/ct/nist_beacon.cfm)

**CONTACT:**

Dr. René Peralta  
(301) 975-8702  
[rene.peralta@nist.gov](mailto:rene.peralta@nist.gov)

## Entropy as a Service (EaaS)

The security of cryptography today depends on having strong keys and keeping them secret. The ability to generate strong cryptographic keys is directly related to having access to unpredictable random data, but generating truly unpredictable random data on computing devices is hard and unreliable. As a result, weak keys are widely used in cryptographic applications compromising the security of sensitive data protected by them with potentially disastrous consequences.

A primary goal of this project is to provide high-quality, truly unpredictable random data to devices on the Internet to enable them to generate strong cryptographic keys and attest the strength of the keys used to protect data in transit or at rest, thereby enabling cryptographic system strength attestation. Achieving this goal would provide a solid basis for addressing the problems targeted by Cryptographic System Validation (see the next section: Validated Programs, the first project in this section).

Random data obtained from sources of true randomness that are based on unpredictable physical phenomena, such as quantum effects, is much better suited for cryptographic applications. CSD is collaborating with the NIST Physical Measurement Laboratory (PML) to build a quantum source. The aim is to use quantum effects to generate sequences that are guaranteed to be unpredictable, even if an attacker has access to the random source. For more information on this collaboration, see [http://www.nist.gov/pml/div684/random\\_numbers\\_bell\\_test.cfm](http://www.nist.gov/pml/div684/random_numbers_bell_test.cfm).

This project aims to develop a system and protocols for obtaining random data with high entropy from one or more remote sources. The high-level architecture is shown in Figure 10 (see next page). The architecture of the Entropy-as-a-Service system consists of two main parts: the client-side and the server-side. The critical components of the system are the quantum device, the EaaS server and a secure device in the client systems capable of providing strong isolation and protection for the cryptographic keys stored inside the device and offering a set of basic cryptographic services.

Client devices mix this data with locally available random data to seed random number generators to generate strong cryptographic keys and other random values independently from the remote sources.



With system architecture and protocols defined, the project team have engaged with industry and academia to obtain feedback on the approach and identify possibilities for collaborative approaches to solving important cybersecurity challenges in the domains of cryptography and supply-chain management, e.g., integrated circuit counterfeiting.

The project team have developed a working prototype and demonstrated it at high-profile cybersecurity forums and academic conferences. The team is continuing to develop the system aiming to stand up a publicly accessible NIST EaaS instance in the near future. In addition, the team is also planning to publish the server and client code on GitHub and invite the public to voluntarily adopt it. Related to this, the project team is planning to work on developing public criteria for reputable EaaS hosts.

## CONTACTS:

Dr. Apostol Vassilev  
(301) 975-3221  
apostol.vassilev@nist.gov

Mr. Harold Booth  
(301) 975-8441  
harold.booth@nist.gov

Mr. Robert Staples  
(301) 975-4578  
robert.staples@nist.gov

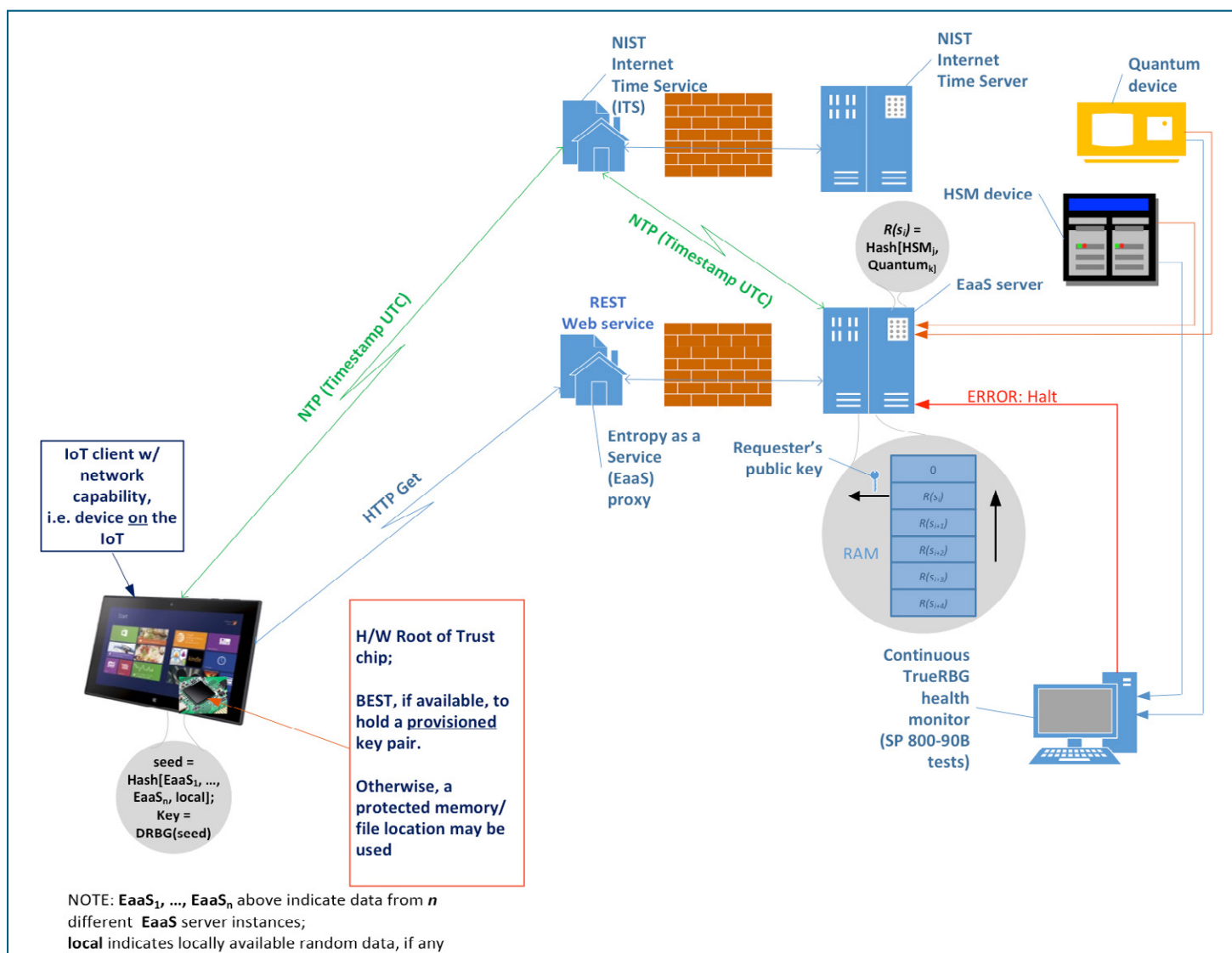


Figure 10: High-level architecture of EaaS

## Wireless and Mobile Security

Today, wireless networks often provide connections for mobile devices using multiple radio technologies. In such a heterogeneous network, a mobile device may switch its connection between different wireless technologies, such as between cellular and WiFi networks. The procedure for conducting such a switch is called a “handover.” Media-independent handover (MIH) is a set of services specified in IEEE 802.21 to assist the handover. When the services provided by the pervasive heterogeneous networks are extended to other applications, such as Smart Grid applications, the MIH needs to be processed by a group of wireless nodes, such as smart meters, for balancing the network load and for reliability. In this case, the information may need to be delivered to a group of smart meters using a multicast message, which is used to deliver the information. That is, the multicast message is sent from one point-of-service (PoS) to multiple wireless nodes. In some of the application environments, such as sensor networks, the groups are formed dynamically; new nodes can be added to the group, and some nodes in the group may need to be removed. Such groups are managed through multicast signals.

Amendment 2 of IEEE 802.21 provides protection mechanisms for unicast messages – mechanisms that protect messages between a PoS and a single mobile node. In FY 2015, CSD continued work with IEEE 802.21 to develop security solutions for group management in Task Group D of IEEE 802.21. The solutions, specified in IEEE 802.21 Amendment 4, include the mechanisms to distribute group keys and for the protection of multicast messages. Amendment 4 of IEEE 802.21 was published in FY 2015.

In FY 2016, CSD will continue to contribute to a broader scope of IEEE 802 wireless standards.

### CONTACT:

Dr. Lily Chen  
(301) 975-6974  
lily.chen@nist.gov

## Authentication

To support OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, NIST’s CSD developed SP 800-63, *Electronic Authentication Guideline*. The OMB memorandum defines four levels of assurance that a federal agency must select, based on a risk assessment to determine the impact of an authentication failure. This guideline covers the remote authentication of users (such as private individuals) interacting with government IT systems

over the Internet. It defines technical requirements for each of the four levels of assurance in the areas of identity proofing, tokens, credential binding, management processes, authentication protocols and assertion characteristics. Since the initial release of SP 800-63, the CSD has released two revisions to address changes in modern technology and lessons learned from practical implementations by federal departments and agencies.

Several recent developments have an impact on the way that agencies fulfill their e Authentication requirements:

- Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, issued by the administration in October 2014, requires “...that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate.” (see <http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions>)
- CSD published *The Framework for Improving Critical Infrastructure Cybersecurity* in February 2014 in response to Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity* (for the Framework, see <http://www.nist.gov/cyberframework/>; for the EO 13636, see <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>). The accompanying roadmap cites the need for NIST to “...conduct identity and authentication research complemented by the production of Special Publications that support improved authentication practices.” (see <http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf>)
- The National Strategy for Trusted Identities in Cyberspace (NSTIC), which was released in 2011, charts a course for both public and private sectors to collaborate to raise the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions through an Identity Ecosystem (see <http://www.nist.gov/nstic/>). NSTIC calls for the Federal Government to “lead by example and implement the Identity Ecosystem for the services it provides internally and externally.” As the Identity Ecosystem starts to take shape, NIST guidelines should reflect and support it.

In addition, market forces have resulted in an inflexion point in how departments and agencies authenticate users. NIST and our private sector partners have observed that some public and private sector identity assurance standards have become outdated or have simply not been adopted.

Specifically, SP 800-63 was originally written to address an online world that is much different than today. Innovation has offered new perspectives in how trusted identities can be established. Practical implementations of SP 800-63 have informed us of areas of strengths, weaknesses, and techniques not utilized by federal agencies or the private sector. In addition, federal agencies are the only organizations required to follow NIST SPs. However, as the Federal Government evolves to accept credentials offered by private sector organizations, the applicability of SP 800-63 has expanded beyond agency use. NIST has an obligation to service the expansion of the original SP 800-63 target.

Therefore, in April of 2015, NIST issued a call for comments on the current published version, SP 800-63-2, in order to identify specific topics that could be addressed in a future revision of SP 800-63 (see [http://csrc.nist.gov/groups/ST/eauthentication/sp800-63-2\\_call-comments.html](http://csrc.nist.gov/groups/ST/eauthentication/sp800-63-2_call-comments.html)). NIST received over 40 submissions from individuals, academia, and the public and private sectors. Over 300 distinct comments were identified from these submissions. In addition to the comments that NIST received, vulnerabilities have been discovered in existing online authentication services, specifically in the area of remote identity proofing, which has warranted an accelerated consideration of updated guidance for the Federal Government.

In FY 2016, CSD expects its authentication work to be driven by the needs of the ongoing rapid expansion of online service delivery, commercially available authentication services, results and metrics from NSTIC pilots, and the availability of multi-factor tokens to consumers. Breaches of personal information and the relative availability of personal information has necessitated that NIST reconsider approaches to identity proofing, both in-person and remotely. The paradigm where the starting assumption was that personal data was hard to find has now changed to one where it is acknowledged that this data is readily available online; existing guidance needs to be adjusted to offer organizations cost-effective, yet secure, identity proofing capabilities. The NSTIC pilots have tested innovative alternatives to high-assurance remote proofing, necessitating that SP 800-63 be considerate of these advances in the marketplace. In addition, commercial advances in physical document validation and verification, the proliferation of high-resolution video cameras on commodity computing devices, including mobile phones, as well as new offerings in the delivery of in-person proofing, will influence potential updates to requirements at all levels of assurance.

As many types of biometric sensors become ubiquitous in personal mobile devices, and more and more individuals leverage biometrics in commercial use cases such as mobile payment and online authentication to private sector services, CSD will re-examine the current position of remote, unattended biometric authentication. The existing publication does allow local biometric authentication to unlock a token – a secure technique currently used by popular mobile handset manufacturers. Yet the comments CSD received reveal that some believe this is insufficient, and that centralized biometric authentication used in single- or multi-factor schemes should be allowed in a future revision. CSD will pursue detailed research in the security of remote biometric authentication, examine the efficacy of standardization efforts related to presentation attack detection, and contemplate the long-term impacts of the en-masse theft of biometrics before expanding the current requirements of SP 800-63-2.

The user experience of online authentication will also be a significant consideration in a potential update of SP 800-63. The CSD has observed that the user experience has a direct relationship with individual uptake of authentication services as well as the overall security of any authentication scheme. While CSD does not intend to weaken requirements to accommodate a favorable user experience, understanding the impact of e-Authentication requirements on the user, and to design requirements that do not degrade security but upgrade the user experience, is imperative.

The CSD, therefore, plans to actively consider revisions to SP 800-63-2 in response to the issues noted above and other issues that can be dealt with in time to assist in the intense ongoing efforts to expand online services.

**For More Information, See:**

<http://csrc.nist.gov/groups/ST/eauthentication/>

**CONTACT:**

Mr. Paul Grassi  
(703) 786-8275  
[paul.grassi@nist.gov](mailto:paul.grassi@nist.gov)



## VALIDATION PROGRAMS

Federal agencies, industry, and the public rely on many of the standards and specifications supported by CSD. Poor implementations of these standards or specifications may render a particular product insecure, potentially placing sensitive information at risk. CSD operates several validation programs that help provide a level of assurance that products meet established security requirements and conform to published specifications. To that end, the Security Testing, Validation, and Measurement Group (STVMG) develops test suites and test methods; provides implementation guidance and technical support to industry forums; and conducts education, training, and outreach programs.

STVMG's validation programs work together with independent laboratories that are accredited by the National Voluntary Laboratory Accreditation Program (NVLAP). Based on the independent laboratory test report and test evidence provided by the labs, the validation programs described below validate the implementation under test. CSD subsequently publishes lists of the validations awarded on public websites.

### Cryptographic System Validation

Current validation programs focus on providing a known level of assurance for cryptographic algorithms and modules. These modules are used within the context of a larger system to provide cryptographic services as a method of protecting the data within the system. As information systems continue to become more complex, the methods used to implement cryptographic services have also increased in complexity. Problems with the use of cryptography are often introduced through the interaction of cryptographic components with the operating environment. This program seeks to specify how cryptographic components are used as part of a defined cryptographic system to solve problems with a measureable level of assurance, and to introduce automated methods of quantifying the level of assurance that has been provided.

In FY 2016, this program will begin the research required to define a reference cryptographic systems architecture and example use cases where cryptographic systems are built from known cryptographic components that cooperate through trust relationships to provide a measureable level of assurance. The architecture should begin at the lowest level with a hardware-based root of trust, and each cryptographic component should be added in successive layers to provide assurance in a systematic way. This should allow the development of tests that would measure the correct implementation of cryptographic components as part of a larger system.

This program will perform research and experimentation in applicable technologies and techniques that will enable the efficient testing of the cryptographic capabilities of each layer, and enable the continuous monitoring capabilities of each cryptographic component, providing the necessary interfaces to establish trust relationships with other cryptographic components. Techniques could include such items as:

- Embedding XML data elements and standard interfaces to query those data elements during the design and implementation of cryptographic components that would enable automated testing capabilities;
- Using cryptographic techniques to embed values into the module that would increase the verifiability and assurance that the module provides; and
- Using industry-based secure development techniques to increase the level of trust inherent in software modules, starting with design and implementation.

Research into this area of cryptographic system validation holds the promise of automating the validation of all cryptographic components, providing a higher assurance with less manual effort. The program will use an approach that was developed for the SCAP product validation effort to embed data elements that instrument the test harnesses used to validate cryptographic systems. This would also provide the instrumentation that could be leveraged to enable a greater level of situational awareness and security measurement, and potentially, to enable continuous monitoring of cryptographic systems.

### CONTACT:

Mr. Michael Cooper  
(301) 975-8077  
michael.cooper@nist.gov

### Cryptographic Programs and Laboratory Accreditation

The Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP) were developed in collaboration between NIST and the Communications Security Establishment (CSE) of Canada to support the respective federal user communities for strong, independently tested, and commercially available cryptographic algorithms and modules. Through these programs, NIST and CSE work with international government, public and private sectors as a part of the cryptographic community to achieve standards-based security and assurance of correct implementation. The goal of these programs is to provide federal agencies

with a security metric to use in procuring and deploying cryptographic modules, and promote the use of validated algorithms and modules by industry and the public. The testing carried out by independent third-party laboratories accredited by NVLAP, and the validations performed by the CAVP and CMVP programs provide this metric. Federal agencies, industry, and the public can choose cryptographic modules and/or products containing cryptographic modules from the CMVP Validated Modules List and have confidence in the claimed level of security and assurance of correct implementation.

Cryptographic algorithm and cryptographic module testing and validation are based on published NIST standards. Since federal agencies are required to use validated cryptographic modules for the protection of sensitive unclassified information, the validated modules and the validated algorithms that the modules contain represent the culmination and delivery of CSD's cryptography-based work to the end user.

The CAVP and the CMVP are separate collaborative programs. The CAVP and the CMVP validate algorithms and modules, respectively, which are used in a wide variety of products, including Internet browsers, radios, smart cards, space-based communications, munitions, security tokens, mobile phones, network and storage devices, and products supporting the Public Key Infrastructure (PKI) and electronic commerce. A module may be a standalone product, such as a virtual private network (VPN) or smart card, or it could be a module embedded in many products, such as a cryptographic-based toolkit. As a result, a small number of modules may be incorporated within hundreds of products. The CAVP validates cryptographic algorithms that may be integrated in one or more cryptographic modules. Figure 11 provides a flow of the CMVP testing and validation process.

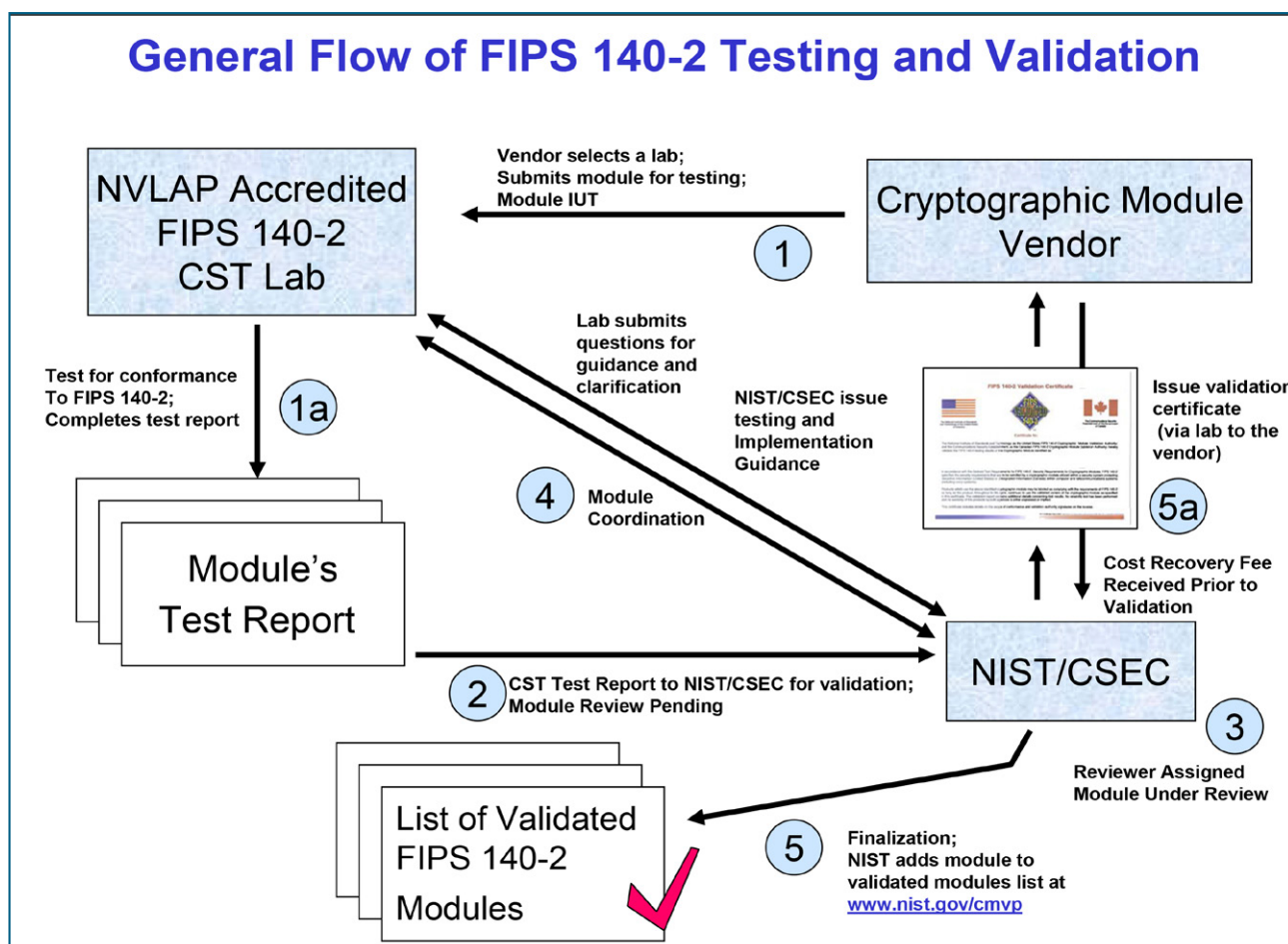


Figure 11: General Flow of FIPS 140-2 Testing and Validation

The CAVP and CMVP validation programs provide documented methodologies for conformance testing through defined sets of security requirements. For the CAVP, the validation system documents are designed for each FIPS-approved or NIST-recommended cryptographic algorithm. See the website for a listing (see <http://csrc.nist.gov/groups/STM/cavp/>). Security requirements for the CMVP are found in FIPS 140-2, *Security Requirements for Cryptographic Modules*, and the associated test metrics and methods in Derived Test Requirements for FIPS 140-2, *Security Requirements for Cryptographic Modules*. The four Annexes to FIPS 140-2 reference the underlying cryptographic algorithm standards or methods. The CMVP-developed Implementation Guidance for FIPS 140-2 and the Cryptographic Validation Program provides programmatic and implementation guidance across all of the referenced documents. The information provided in the Derived Test Requirements (DTR) and Implementation Guidance (IG) documents ensures the repeatability of tests and the equivalency of results across the testing laboratories. The IG provides clarity, consistency of interpretation, and insight for successful conformance testing, validation, and revalidation.

The unique position of the validation programs gives the CAVP and CMVP the opportunity to acquire insight during the validation review activities and results in practical, timely, and up-to-date guidance that is needed by the testing laboratories and vendors to move their modules out to the user community in a timely and cost-effective manner and with the assurance of third-party conformance testing. This knowledge and insight provide a foundation for current and future standards and tools development.

The CMVP reviews the cryptographic module validation requests from the testing laboratories and, as a byproduct of the review, is attentive to emerging and/or changing technologies.

Starting with FY 2015, the Security Testing, Validation, and Measurement (STVM) group created a research team

whose mission is to conduct research to assist developers of cryptographic modules, testing laboratories, and the user community when developing new standards. The insights from this research into the evolution of operating environments and complex systems allow the CMVP to perform research and development on evolving test metrics and methods and future requirements for cryptographic modules.

The CAVP and the CMVP have stimulated the improved quality and security assurance of cryptographic algorithm implementations and modules. By the end of FY 2015, the CMVP had validated and issued a total of 2,380 cryptographic module validation certificates to more than 475 domestic and international vendors. As shown in Figure 12, the CMVP awarded 197 certificates in FY 2015. The left portion of the graphic illustrates the distribution by submission type, based upon the modification scenarios described in the CMVP Implementation Guidance, including:

- 1SUB - Modifications made to hardware, software or firmware components that did not affect any FIPS 140-1 or FIPS 140-2 security relevant items (e.g., a maintenance activity);
- 3SUB - Modifications that include changes that affect some of the FIPS 140-2 security-relevant items and require revalidation, but drew upon previous submissions; and,
- 5SUB - Significant changes to hardware, software, or firmware components and, therefore, were considered a new module requiring full validation testing.

The right portion of the diagram shows the number of certificates awarded, based upon each of the four increasing levels of security specified in the FIPS that may be satisfied by a cryptographic module.

Likewise, to date, the CAVP has issued approximately 19,578 validations, representing the algorithm validations of approximately 17 approved algorithms.

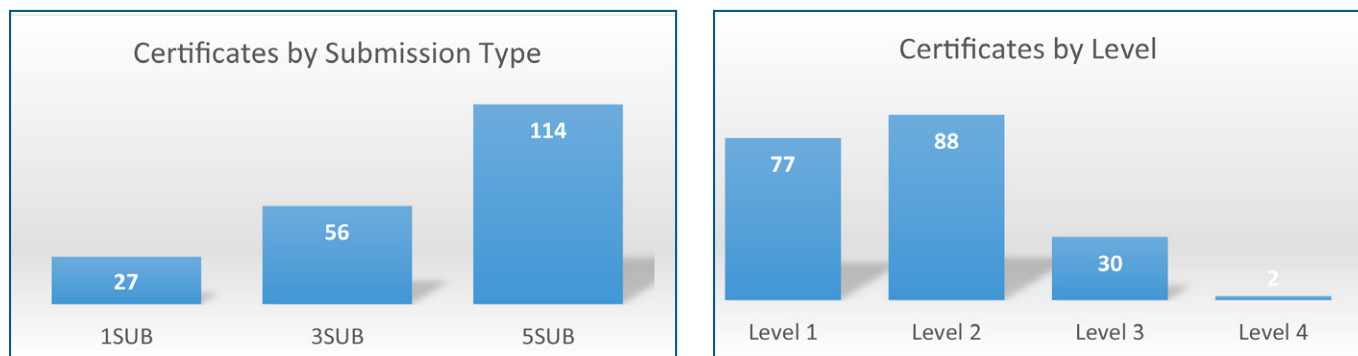


Figure 12: FY 2015 FIPS 140-2 Validations



## CAVP Validation Status By FYs

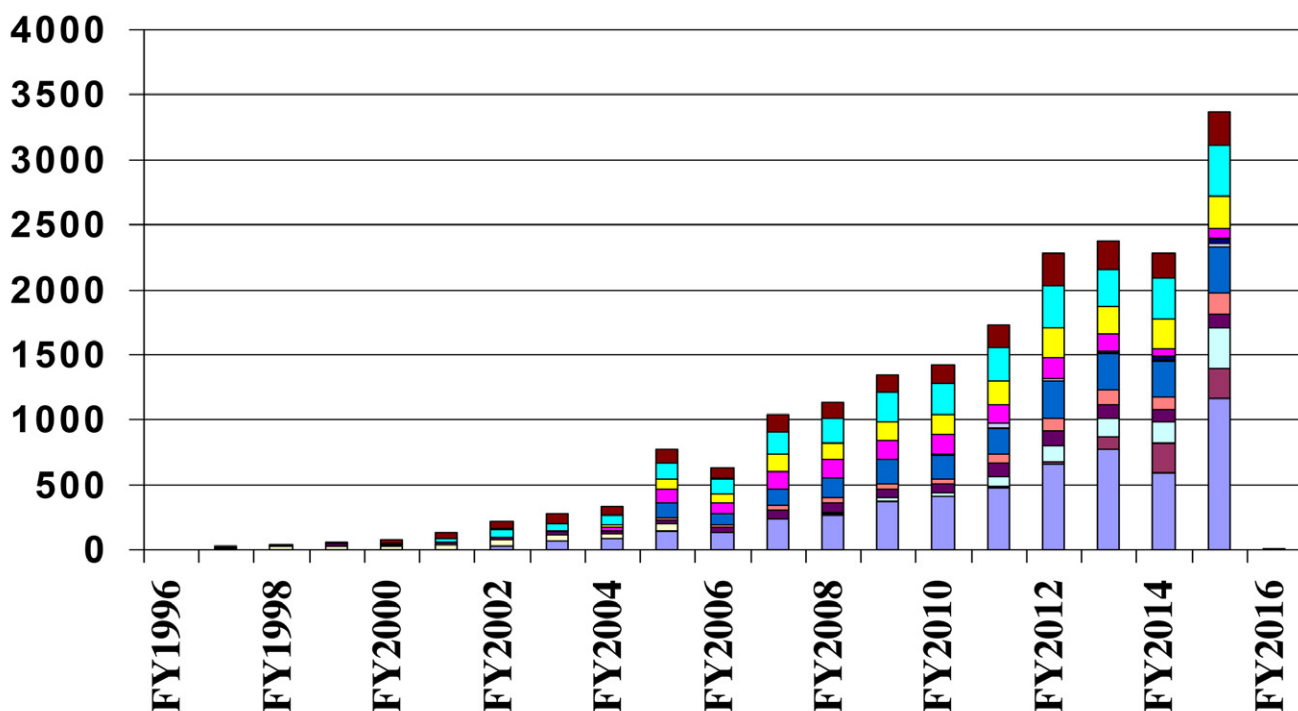


Figure 13: CAVP Validation Status by Fiscal Year

## CAVP Validation Status For FY15

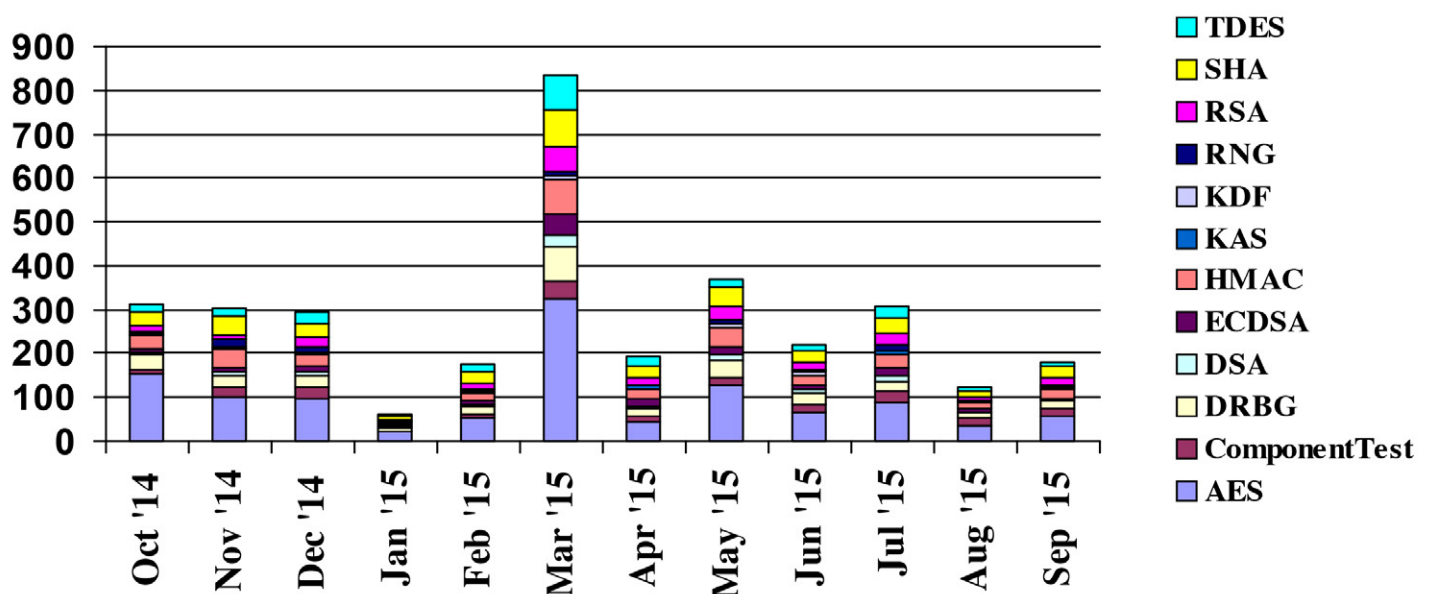


Figure 14: CAVP Validation Status for FY 2015

# CAVP Validated Implementation Actual Numbers

Updated As: Wednesday, October 28, 2015

FiscalYear	AES	Comp.	DES	DSA	DRBG	ECDSA	HKMAC	KAS	KDF	RNG	RSA	SHA	SJ	TDES	Total
FY1996	0	0	2	0	0	0	0	0	0	0	0	0	0	0	2
FY1997	0	0	11	6	0	0	0	0	0	0	0	7	2	0	26
FY1998	0	0	27	9	0	0	0	0	0	0	0	6	0	0	42
FY1999	0	0	30	14	0	0	0	0	0	0	0	12	1	0	57
FY2000	0	0	29	7	0	0	0	0	0	0	0	12	1	28	77
FY2001	0	0	41	15	0	0	0	0	0	0	0	28	0	51	135
FY2002	30	0	44	21	0	0	0	0	0	0	0	59	6	58	218
FY2003	66	0	49	24	0	0	0	0	0	0	0	63	3	73	278
FY2004	82	0	41	17	0	0	0	0	0	28	22	77	0	70	337
FY2005	145	1	54	31	0	14	115	0	0	108	80	122	2	102	774
FY2006	131	1	3	33	0	19	87	0	0	91	63	120	1	83	632
FY2007	238	5	0	63	0	35	127	0	0	137	130	171	1	136	1043
FY2008	271	7	0	77	4	41	158	0	0	137	129	191	0	122	1137
FY2009	373	2	0	71	23	33	193	6	0	142	143	224	1	138	1349
FY2010	406	2	0	70	31	39	179	12	0	150	155	239	0	142	1425
FY2011	474	11	0	102	79	68	201	34	0	148	183	255	0	177	1732
FY2012	654	24	0	121	122	92	283	20	3	157	231	323	1	248	2279
FY2013	778	88	0	106	145	113	276	12	9	132	208	293	0	217	2377
FY2014	594	223	0	95	167	96	276	14	23	63	225	314	0	196	2286
FY2015	1166	226	0	99	320	164	355	32	35	80	243	396	0	256	3372
<b>Total</b>	<b>5408</b>	<b>590</b>	<b>331</b>	<b>981</b>	<b>891</b>	<b>714</b>	<b>2250</b>	<b>130</b>	<b>70</b>	<b>1373</b>	<b>1812</b>	<b>2912</b>	<b>19</b>	<b>2097</b>	<b>19578</b>

Figure 15: CAVP Validated Implementation Actual Numbers

The CAVP issued approximately 3,372 algorithm validations in FY 2015, an increase of over 1,000 validations from the previous year. The increase in validations is attributed to other outside programs now requiring CAVP validated implementations (e.g., NIAP).

The CMVP issued 197 module validation certificates in FY 2015. The number of algorithms and modules submitted for validation continues to grow, representing significant growth in the number of validations expected to be available in the future.

## For More Information, See:

<http://csrc.nist.gov/groups/STM>

CMVP Implementation Guidance, G.8

<http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf>

## CMVP CONTACTS:

Ms. Jennifer Cawthra  
(301) 975-8514  
[jennifer.cawthra@nist.gov](mailto:jennifer.cawthra@nist.gov)

Dr. Apostol Vassilev  
(301) 975-3221  
[apostol.vassilev@nist.gov](mailto:apostol.vassilev@nist.gov)

## CAVP CONTACT:

Ms. Sharon Keller  
(301) 975-2910  
[sharon.keller@nist.gov](mailto:sharon.keller@nist.gov)

## Automated Security Testing and Test Suite Development

The CAVP utilizes the requirements and specifications of NIST standards (i.e., FIPS and Special Publications) to develop algorithm validation test suites and automated security testing. The CAVP is responsible for providing assurance that the cryptographic algorithm implementations contained in cryptographic modules are implemented according to the specifications in the standards. The CAVP accomplishes this by designing and developing conformance testing specific to each cryptographic algorithm.

The conformance testing consists of a suite of validation tests for each approved cryptographic algorithm. These validation tests exercise the algorithmic requirements and mathematical formulas detailed in the algorithm to assure that the detailed specifications are implemented correctly and completely. If the implementer deviates from the specifications in the standard or excludes any part of these specifications or requirements, the validation test will detect the deviations and fail. The validation testing will indicate that the algorithm implementation does not function properly or is incomplete.

The cryptographic algorithm validation tests designed and developed by the CAVP are used by independent third-party laboratories accredited by the NVLAP. The laboratory works with vendors to validate their cryptographic algorithm implementations. The suite of validation tests for each algorithm ensures the repeatability of tests and the equivalency of results across the testing laboratories.

There are several types of validation tests, all designed to satisfy the testing requirements of the cryptographic algorithms and their specifications. These include, but are not limited to, Known-Answer Tests, Monte Carlo Tests, and Multi-Block Message Tests. The Known-Answer Tests are designed to examine the individual components of the algorithm by supplying known values to the variables

and verifying the expected result. Negative testing is also performed by supplying known incorrect values to assure that the implementation recognizes values that are not allowed. The Monte Carlo Test is designed to exercise the entire implementation under test (IUT). This test is designed to detect the presence of implementation flaws that are not detected with the controlled input of the Known-Answer Tests. The types of implementation flaws detected by this validation test include pointer problems, insufficient allocation of space, improper error handling, and incorrect behavior of the IUT. The Multi-Block Message Test (MMT) is designed to test the ability of the implementation to process multi-block messages, which requires the chaining of information from one block to the next.

During the last few years, the CTG has expanded its publications to contain not only the algorithm's specifications, but also requirements for an algorithm's use. Many of these usage requirements do not fall within the scope of the CAVP, because the CAVP focuses on the correctness of the instructions within the algorithm's boundary. If these additional algorithm usage requirements are not considered applicable to the algorithm's implementation, they cannot be tested at the algorithm level by the CAVP, but may be tested by the Cryptographic Module Validation Program (CMVP) if the requirements are considered applicable to the cryptographic module. However, some of these usage requirements may be considered to be outside the scope of both the algorithm implementation and cryptographic module. In this latter case, the fulfillment of the requirements is the responsibility of entities using, installing, or configuring applications or protocols that use the cryptographic algorithms. For example, depending on the design of a cryptographic module, it may not be possible for the module to determine whether a specific key is used for multiple purposes, a situation that is strongly discouraged.

The CAVP currently has algorithm validation testing for the following cryptographic algorithms:

TABLE 1: CRYPTOGRAPHIC ALGORITHMS & NIST TECHNICAL DOCUMENTS (FIPS & SPS)	
CRYPTOGRAPHIC ALGORITHM/COMPONENT	FEDERAL INFORMATION PROCESSING STANDARD (FIPS) OR SPECIAL PUBLICATION (SP)
Triple Data Encryption Standard (TDES)	SP 800-67, <i>Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher</i> , and
	SP 800-38A, <i>Recommendation for Block Cipher Modes of Operation—Methods and Techniques</i>
Advanced Encryption Standard (AES)	FIPS 197, <i>Advanced Encryption Standard</i> , and
	SP 800-38A, <i>Recommendation for Block Cipher Modes of Operation—Methods and Techniques</i>

**TABLE 1 (CONT.): CRYPTOGRAPHIC ALGORITHMS & NIST TECHNICAL DOCUMENTS (FIPS & SPS)**

<b>CRYPTOGRAPHIC ALGORITHM/COMPONENT</b>	<b>FEDERAL INFORMATION PROCESSING STANDARD (FIPS) OR SPECIAL PUBLICATION (SP)</b>
Digital Signature Algorithm (DSA)	FIPS 186-2, <i>Digital Signature Standard (DSS)</i> , with change notice 1
	FIPS 186-4, <i>Digital Signature Standard (DSS)</i>
Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS 186-2, <i>Digital Signature Standard (DSS)</i> , with change notice 1 and ANS X9.62
	FIPS 186-4, <i>Digital Signature Standard (DSS)</i> , and ANS X9.62
RSA algorithm	FIPS 186-4, <i>Digital Signature Standard (DSS)</i>
	ANS X9.31 and Public Key Cryptography Standards (PKCS) #1 v2.1: RSA Cryptography Standard-2002
Hashing algorithms SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256	FIPS 180-4, <i>Secure Hash Standard (SHS)</i>
Random number generator (RNG) algorithms	FIPS 186-2 Appendix 3.1 and 3.2; ANS X9.62 Appendix A.4
Deterministic Random Bit Generators (DRBG)	SP 800-90A, <i>Recommendation for Random Number Generation Using Deterministic Random Bit Generators</i>
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198-1, <i>The Keyed-Hash Message Authentication Code (HMAC)</i>
Cipher-based Message Authentication Code (CMAC) Mode for Authentication	SP 800-38B, <i>Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication</i>
Counter with Cipher Block Chaining-Message Authentication Code (CCM) Mode	SP 800-38C, <i>Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality</i>
GCM and GMAC Modes	SP 800-38D, <i>Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC</i>
XTS-AES Mode	SP 800-38E, <i>Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Block-Oriented Storage Devices</i>
Key Wrapping	SP 800-38F, <i>Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping</i>
DH and MQV Key Agreement Schemes and Key Confirmation	SP 800-56A, <i>Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography</i> , dated March 2007
All of SP 800-56A schemes without the Key Derivation Functions (KDF)	SP 800-56A, Key Derivation Functions for Key Agreement Schemes: All sections except Section 5.8
All of SP 800-56A schemes without the Key Derivation Functions (KDF)	SP 800-56A, Section 5.7.1.2 Elliptic Curve Cryptography Cofactor Diffie-Hellman (ECC CDH) Primitive Testing
Key-Based Key Derivation functions (KBKDF)	SP 800-108, <i>Recommendation for Key Derivation using Pseudorandom Functions</i>



**TABLE 1 (CONT.): CRYPTOGRAPHIC ALGORITHMS & NIST TECHNICAL DOCUMENTS (FIPS & SPS)**

CRYPTOGRAPHIC ALGORITHM/COMPONENT	FEDERAL INFORMATION PROCESSING STANDARD (FIPS) OR SPECIAL PUBLICATION (SP)
Application-Specific Key Derivation functions (ASKDF) (includes the KDFs used by IKEv1, IKEv2, TLS, ANS X9.63-2001, SSH, SRTP, SNMP, and TPM)	SP 800-135 (Revision 1) <i>Recommendation for Existing Application Specific key Derivation Functions</i>
Component test – ECDSA Signature Generation of a hash value (This component test verifies the signing of a hash-sized input. It does not verify the hashing of the original message to be signed.)	FIPS 186-4, <i>Digital Signature Standard (DSS)</i> , and ANS X9.62
Component test – RSA PKCS#1.5 Signature Generation of encoded message EM (This component test verifies the signing of an EM. It does not verify the formatting of the EM.)	FIPS 186-4, <i>Digital Signature Standard (DSS)</i> , and Public Key Cryptography Standards (PKCS) #1 v2.1: RSA Cryptography Standard-2002
Component test – RSA PKCS#1 PSS Signature Generation of encoded message EM (This component test verifies the RSASP1 function.)	SP 800-56B, <i>Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography</i> , August 2009, Section 7.1.2

In FY 2016, the CAVP expects to add algorithm validation testing for:

- FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*, August 2015;
- SP 800-56C, *Recommendation for Key Derivation through Extraction-then-Expansion*, November 2011;
- SP 800-132, *Recommendation for Password-Based Key Derivation Part 1: Storage Applications*, December 2010; and
- SP 800-56A Revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, May 2013.

#### For More Information, See:

<http://csrc.nist.gov/groups/STM/cavp>

#### CONTACTS:

Ms. Sharon Keller  
(301) 975-2910  
[sharon.keller@nist.gov](mailto:sharon.keller@nist.gov)

Ms. Elaine Barker  
(301) 975-2911  
[elaine.barker@nist.gov](mailto:elaine.barker@nist.gov)

## Security Content Automation Protocol (SCAP) Validation Program

The SCAP Validation Program performs conformance testing to ensure that products correctly implement SCAP as defined in SP 800-126 Revision 2, *The Technical Specification for the Security Content Automation Protocol*

(SCAP): *SCAP Version 1.2*. Conformance testing is necessary because SCAP is a complex collection of eleven individual specifications that work together to support various use cases. A single error in product implementation could result in undetected vulnerabilities or policy noncompliance within an organization's networks.

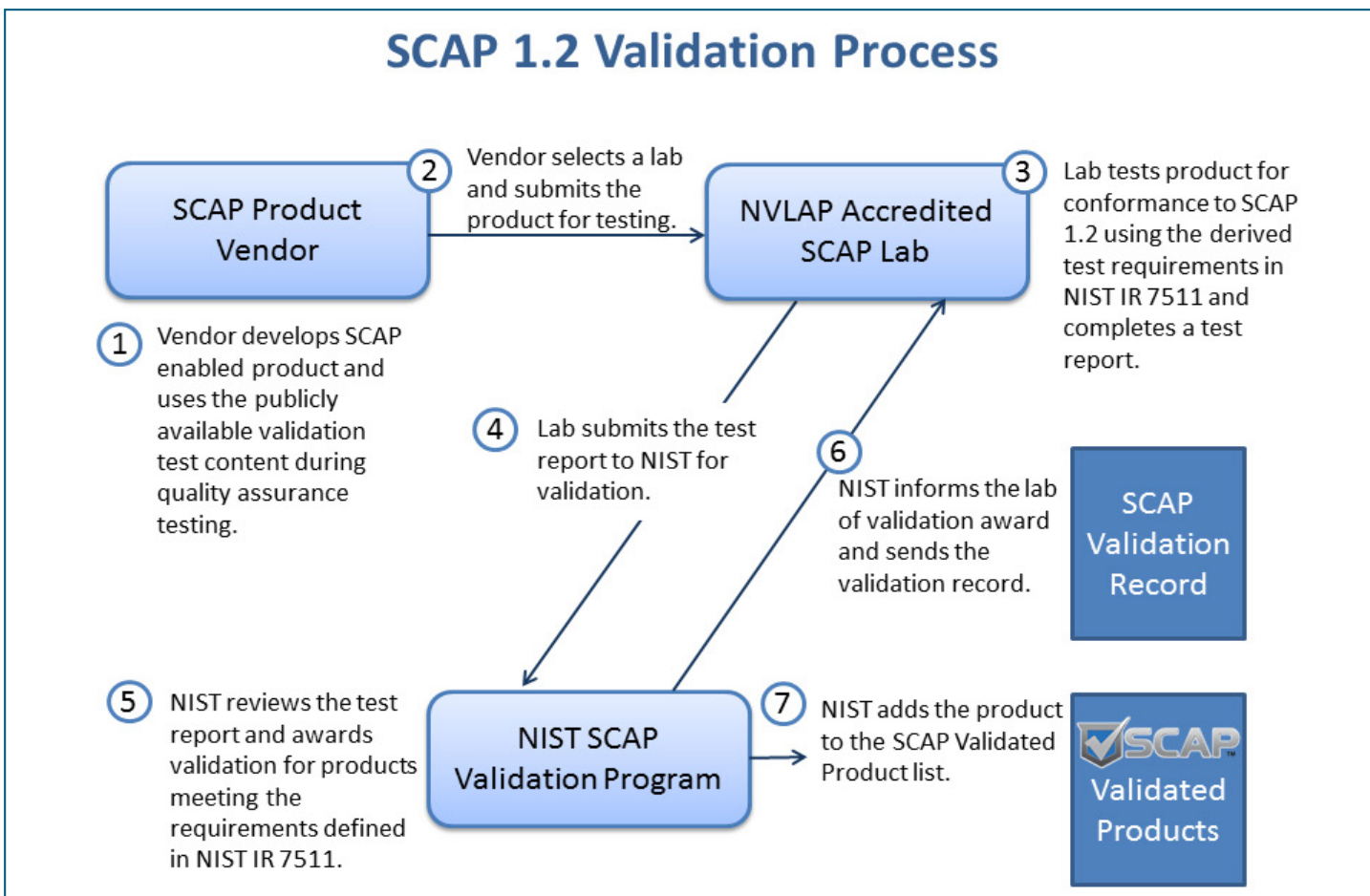


Figure 16: SCAP 1.2 Validation Process

The test requirements for SCAP 1.2 are defined in NISTIR 7511, *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements*. In general, vendors may opt for product validation for one or more SCAP capabilities or operating systems. Currently, the program offers testing on Microsoft Windows and Red Hat Enterprise Linux platforms. Figure 16 illustrates the SCAP 1.2 Validation Process. The validation process starts when a vendor voluntarily submits an SCAP-enabled product to an NVLAP-accredited laboratory. Once the lab completes product testing, the lab submits a test report to the SCAP Validation Program at NIST for review. NIST reviews the test report and awards a validation if all requirements have been met. Once a validation is awarded, the SCAP Validation Record is sent to the lab, and the information about the newly validated product is posted on the SCAP Validated Products web page.

The SCAP Validation Program resources web page provides the public with a centralized location for all resources and information necessary for preparing products for SCAP 1.2 validation. Resources include: documentation, a list of Frequently Asked Questions (FAQ), the SCAP validation-test content, and tools for validating and processing SCAP data streams. The SCAP validation-test content should be used by vendors for quality assurance testing prior to entering formal SCAP testing with an NVLAP-accredited laboratory. The open-source tools that are available for download may be used by SCAP content authors for testing SCAP source content. The SCAP Content Validation Tool (SCAPVal) may be used to determine if the content conforms to the SCAP specification. Open-source SCAP reference implementation tools, such as the SCAP Reference Implementation Tool, may be used to process SCAP data streams.

End users may use information on the SCAP Validation web page to learn about SCAP validation and find products that have been awarded validations. The validation records that are posted on the SCAP Validated Products page identify the product versions that were tested in the laboratory, along with details about each validation, such as the tested platforms, SCAP capabilities, the validation test suite version, and the lab that performed the product test.

In FY 2015, five products successfully completed testing and were awarded validations, bringing the total number of SCAP 1.2-validated products to twelve. This provides coverage for 80 percent of the market space. Several products are in various stages of validation testing and are expected to be awarded validations in FY 2016. The current list of SCAP 1.2-validated products may be found on the SCAP Validated Products list at <https://nvd.nist.gov/SCAP-Validated-Tools>.

In FY 2016, the SCAP Validation Program plans to expand the validation test suite, adding new operating system support and introducing module testing. SCAP module testing enables the “SCAP Inside” labeling program. Products using the “SCAP Inside” label have incorporated an SCAP-validated module; however, the consumer product as a whole has not completed validation testing by an NVLAP accredited laboratory. Additions to the SCAP Validation Program will be defined in NISTIR 7511 Revision 4.

#### **For More Information, See:**

<http://scap.nist.gov/validation>

#### **CONTACT:**

Ms. Melanie Cook  
(301) 975-5259  
[melanie.cook@nist.gov](mailto:melanie.cook@nist.gov)

## **IDENTITY MANAGEMENT**

### **NIST Personal Identity Verification Program (NPIVP)**

The objective of the NIST Personal Identity Verification Program (NPIVP) is to validate PIV components for conformance to the specifications in FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, and its companion documents. The two PIV components that come under the scope of NPIVP are the PIV Smart Card Application and the PIV Middleware. NPIVP test facilities that perform the two types of tests are the Cryptographic and Security Testing (CST) Laboratories that have been accredited by the NVLAP. As of September 2015, there were nine such facilities (see [http://csrc.nist.gov/groups/SNS/piv/npivp/testing\\_facilities.html](http://csrc.nist.gov/groups/SNS/piv/npivp/testing_facilities.html)).

The interface specifications for the PIV Smart Card Application and PIV Middleware are found in a FIPS 201-associated document, namely, SP 800-73-4, *Interfaces for Personal Identity Verification*. The conformance tests for these specifications are detailed in SP 800-85A-2, *PIV Card Application and Middleware Interface Test Guidelines*. To implement these tests and to generate conformance test reports, CSD also developed an integrated toolkit called “PIV Interface Test Runner,” which conducts tests on both PIV Card Application and PIV Middleware products, and provides the toolkit to accredited NPIVP test facilities.

In addition, NPVP is closely involved in ensuring that all changes in PIV companion documents, such as SP 800-73-4, SP 800-76-2, *Biometric Specifications for Personal Identity Verification*, and SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, are fully reflected in the updated versions of the conformance test documents, SP 800-85A-2 and SP 800-85B, as well as in the “PIV Interface Test Runner” toolkit. Currently, the NPVP team is guiding the development of the “PIV Interface Test Runner” toolkit for validating PIV Card application and PIV Middleware products for conformance to the specifications in SP 800-73-4, SP 800-76-2 and SP 800-78-4. In FY 2015, Phase I changes to PIV Interface Test Runner were completed, and NPVP performed acceptance testing.

#### For More Information, See:

<http://csrc.nist.gov/groups/SNS/piv/npivp>

## CONTACTS:

Dr. Ramaswamy Chandramouli (301) 975-5013 mouli@nist.gov	Ms. Hildegard Ferraiolo (301) 975-6972 hildegard.ferraiolo@nist.gov
--	---

## Personal Identity Verification (PIV) and FIPS 201 Revision Efforts



**Figure 17: Government Employees Use PIV Cards for Facility Access**

In response to Homeland Security Presidential Directive-12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*, FIPS 201, *Personal Identity Verification (PIV) of Federal Employees*

and *Contractors*, was developed and was approved by the Secretary of Commerce in February 2005. HSPD-12 called for the creation of a new identity credential for federal employees and contractors. FIPS 201 is the technical specification for both the PIV identity credential and the PIV system that produces, manages, and uses the credential. Within NIST’s Information Technology Laboratory (ITL), this work is a collaborative effort of the Information Access Division (IAD) and CSD. CSD activities in FY 2015 directly supported the recently revised FIPS 201-2 by updating the relevant publications associated with FIPS 201-2 and by developing two new publications. CSD performed the following activities during FY 2015 in support of HSPD-12:

- Published SP 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials*, in December 2014. SP 800-157 defines the technical details for implementing and deploying derived PIV credentials on mobile devices, such as smart phones and tablets. As intended by FIPS 201-2, a derived PIV credential is a PIV credential that can be provisioned directly to a mobile device to enable remote enterprise access from the device. The use of Derived PIV Credentials greatly improves the usability of electronic authentication from mobile devices to remote IT resources, while at the same time maintaining the goals of HSPD-12 for common identification that is secure, reliable, and interoperable government wide.
- Organized and hosted a workshop in March 2015 on upcoming Special Publications supporting FIPS 201-2 (PIV). The event drew over 160 in-person attendees and about 75 webcast remote attendees from government, industry, and academia representing a wide range of implementers and professionals in cybersecurity and physical security. Topics covered included physical access control with the PIV Card, PIV cardholder interagency record exchange, and derived PIV credentials.
- Published SP 800-73-4, *Interfaces for Personal Identity Verification*, in June 2015, after two public comment periods. The three-part SP details the new, optional PIV Card capabilities introduced in FIPS 201-2, including a virtual contact interface (VCI), a secure channel protocol, and an on-card biometric comparison mechanism. SP 800-73-4 also requires new PIV Cards to enforce a minimum PIN length of six digits.
- Published SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, in June 2015, after two public comment periods. The document has been modified to align with SP 800-73-4, and



includes the addition of new algorithms and key sizes for the secure messaging protocol. Cryptographic algorithm validation testing requirements were also added.

- Published Draft SP 800-85A-4, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)*, in June 2015, to align the testing requirements with FIPS 201-2, SP 800-73-4, and SP 800-78-4.
- Published NISTIR 7863, *Cardholder Authentication for the PIV Digital Signature Key*, in June 2015. The document provides clarification for the requirement in FIPS 201-2 that a PIV cardholder perform an explicit user action prior to each use of the digital signature key stored on the card. NISTIR 7863 clarifies the requirement for “explicit user action” and specifies a range of PIN caching options that maintains the goal of “explicit user action” while adhering to a consistent and reliable level of security.
- Published SP 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, in July 2015. The document incorporates changes required by FIPS 201-2 to accredit PIV Card Issuers and includes a set of issuer controls for Derived PIV Credentials Issuers.

In FY 2016, CSD will continue to focus on updating the relevant publications associated with FIPS 201-2, including SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, and developing two new publications: SP 800-156, *Representation of PIV Chain-of-Trust for Import and Export*, and SP 800-166, *Guidelines for Testing Derived Personal Identity Verification (PIV) Credentials*. CSD will also continue to provide technical and strategic inputs to the PIV-related initiatives.

#### For More Information, See:

<http://csrc.nist.gov/groups/SNS/piv/>

## CONTACTS:

Ms. Hildegard Ferraiolo  
(301) 975-6972  
[hildegard.ferraiolo@nist.gov](mailto:hildegard.ferraiolo@nist.gov)

Dr. David Cooper  
(301) 975-3194  
[david.cooper@nist.gov](mailto:david.cooper@nist.gov)

Dr. Ramaswamy Chandramouli  
(301) 975-5013  
[mouli@nist.gov](mailto:mouli@nist.gov)

## RESEARCH IN EMERGING TECHNOLOGIES

### Secure Development Toolchain Competitions

Many security weaknesses in federal information systems stem from software security vulnerabilities induced by software flaws present in current-generation software products. CSD tracks software security vulnerabilities (in the National Vulnerability Database), seeks techniques for the measurement of security vulnerabilities, and also seeks techniques to reduce the impact and prevalence of security vulnerabilities in newly developed products or in new versions of existing products.

One approach to reducing the number of security vulnerabilities in software is to improve the development tools that are available. By identifying languages and software development tools that support a reduction of vulnerabilities and, by stimulating the creation of better tools and tool usage techniques, the approach should help developers produce applications with fewer vulnerabilities. While it is impossible to assure the total absence of security vulnerabilities in this way, it might well be possible to rule out specific, significant classes of vulnerabilities that today provide the basis for many serious exploits.

CSD is developing an empirical, competitive approach to finding the most effective and usable combinations of tools to produce software systems that are relatively free of exploitable vulnerabilities. Multiple competitions are planned that will be based on an idea developed during the *Designing a Secure Systems Engineering Competition Workshop* that was conducted by National Science Foundation in 2010. The workshop proposed a competition for the development of a set of tools to help non-security-expert developers to rapidly build a significant application with zero vulnerabilities, as detected by an extensive public test suite.

The participants in the planned competitions would implement software systems to solve challenge problems using software development tool chains (“toolchains”) of their own choosing, within specified time periods. The toolchains may include existing technologies (e.g., existing software libraries and frameworks, code generators, reusable source code, or bug-finding tools), novel technologies, or any combination thereof. Each competition would apply a time pressure by simulating a deadline in the software development process, increasing the likelihood of an introduction of security flaws. The objective of the toolchains will be to detect or prevent security flaws while still supporting a quick-paced software development of applications with

rich feature sets. Through the demonstration of security flaw avoidance in a time-constrained setting, CSD seeks to show that wide-scale improvements in the overall security of software products can be realized without sacrificing time-to-market. The competitions, which will be open to all interested parties, will aim to provide a level playing field for the application and measurement of the full spectrum of commercial and research software development, composition, and reuse techniques.

In FY 2015, CSD and its contractors developed 8 challenge problems for the competition. A challenge problem is comprised of three parts: 1) a functional specification of a program to develop (during the competition), 2) a security policy that the program must enforce, typically including confidentiality and integrity requirements, and 3) a challenge-problem-specific test suite including 20 fully-automated pass/fail functionality tests, 20 fully-automated pass/fail security tests, and extensive application of random inputs (i.e., fuzz testing). The challenge problems span three initial program types: command-line interface programs, mobile applications (i.e., cell phone apps), and web applications (browser-based apps). In FY 2015, CSD and its contractors also developed a testing infrastructure for the competition and performed testing to exercise the tools and to assess the suitability of the challenge problems.

In FY 2016, CSD plans to re-engineer portions of the testing infrastructure in response to issues uncovered by testing, to perform a second round of testing, and to publicly announce the first toolchain competition.

## CONTACTS:

Mr. Lee Badger (301) 975-3176 lee.badger@nist.gov	Mr. Christopher Johnson (301) 975-3247 christopher.johnson@nist.gov
---	---

## Cloud Computing and Virtualization

The model for Cloud Computing is defined in SP 800-145, *The NIST Definition of Cloud Computing*. Virtualization is a foundational technology that facilitates the use of a computing infrastructure for cloud-computing services. At the core of a virtualized infrastructure is the virtualized host that provides an abstraction of the hardware (e.g., CPU, memory) and that enables multiple computing stacks (comprised of the operating system, middleware, and applications) to be run on a single physical machine, creating dynamically provisioned, elastic compute resources. The efficiency of such a dynamic and distributed processing environment is counter-balanced by the interoperability, portability, and security challenges inherent in this

computing environment. CSD is working in parallel on several projects (introduced below) that aim to accelerate the Federal Government's adoption of secure cloud computing. CSD subject matter experts collaborate with national and international standards setting organizations, and both the public and private sectors in developing security, interoperability and portability standards and guidance.

## CSD Role in the NIST Cloud Computing Program

During FY 2015, the NIST Cloud Computing Team continued to promote the development of publications, national and international standards, and specifications in support of the U.S. Government's (USG) effective and secure use of cloud computing, as well as providing technical guidance to federal agencies for secure and effective cloud-computing adoption. CSD supports many of the technical standards activities hosted by the NIST Cloud Computing Program, with a particular focus on cloud-computing security and forensic science. Activities include the leading role for the development of the following documents:

- SP 800-173, *Guide for Applying the Risk Management Framework to Cloud-based Federal Information Systems* (draft). This publication provides guidance in using the Risk Management Framework described in SP 800-37 Revision 1 to issue an authorization to operate for cloud-based information systems. The draft document will be posted for public comment in the first quarter of FY 2016.
- SP 800-174, *Security and Privacy Controls for Cloud-based Federal Information Systems* (internal draft). The document will provide a cloud overlay of the SP 800-53 Revision 4 security controls for cloud-based ecosystems.
- Define the cloud forensics use cases that address the top four challenges identified in NISTIR 8006, *NIST Cloud Computing Forensic Science Challenges*.

CSD staff members organized the security and forensics tracks of the eighth *NIST Cloud Computing Forum and Workshop*, which was held in July 2015.

In support of U.S. cloud-computing mandates, CSD staff members provided leadership for several public cloud working groups operating under the NIST Cloud Computing Program. These working groups focus on meeting the high-priority requirements described in SP 500-293, *U.S. Government Cloud Computing Technology Roadmap*.

CSD staff chaired or co-chaired several significant cloud computing efforts in 2015:

- Co-Chaired the NIST Cloud Computing Security Working Group and led the working group on the development of SP 800-173, *Guide for Applying the Risk Management Framework to Cloud-based Federal Information Systems*; SP 800-174, *Security and Privacy Controls for Cloud-based Federal Information Systems* (both described on previous page); and on researching the most suitable approach to a structured representation of the SP 800-53 Revision 4 security and privacy controls.
- Co-Chaired the NIST Cloud Computing Forensic Science Working Group and led the development of cloud forensics use cases that document the top four high priority challenges identified in NISTIR 8006.
- Co-Chaired the NIST Cloud Computing Interoperability and Portability Working Group and addressed issues facing cloud computing with respect to interoperability and portability, standards, and common and functional terminologies. The working group's activities were ceased in mid FY 2015.

CSD staff members participated in various standards development organizations, all listed in the section of this report dedicated to international standards.

In FY 2015, CSD members of the NIST cloud-computing team continued research in key areas of cloud security, cloud interoperability and portability, cloud metrics, cloud services, and cloud Service Level Agreements (SLAs). They also presented the results of cloud-computing research and development, introduced the standards and specifications under development, and provided the status of the NIST Cloud-Computing Program in a variety of domestic and international conferences and workshops. CSD staff continues to engage industry and federal agencies for inputs and collaborative work through working groups, publications, and networking.

#### For More Information, See:

<http://www.nist.gov/itl/cloud>

#### CONTACT:

Dr. Michaela Iorga  
(301) 975-8431  
[michaela.iorga@nist.gov](mailto:michaela.iorga@nist.gov)

## Policy Machine – Leveraging Access Control for Cloud Computing

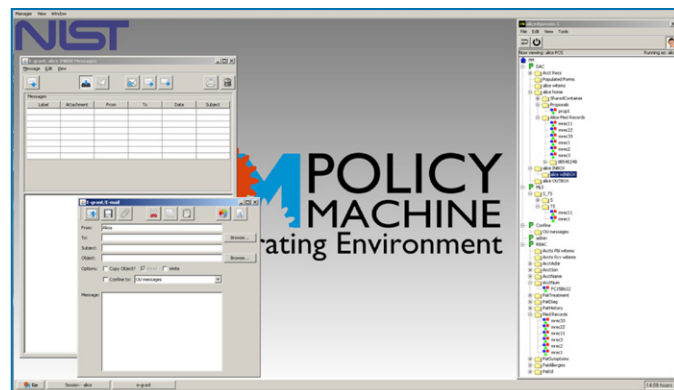


Figure 18: Policy Machine Operating Environment

In FY 2015, CSD continued the research and development of a virtualization utility for enterprise-wide controlled delivery of Cloud data services through Access Control. This included the publication of a revised Policy Machine specification as NISTIR 7987 Revision 1, *Policy Machine: Features, Architecture, and Specification*, in September 2015.

NIST and other members of an Ad Hoc INCITS working group are developing a three-part Policy Machine standard under the title of *Next Generation Access Control (NGAC)*, under three sub-projects:

- Project 2193-D: *Next Generation Access Control – Implementation Requirements, Protocols and API Definitions*;
- Project 2194-D: *Next Generation Access Control – Functional Architecture*; and
- Project 2195-D: *Next Generation Access Control – Generic Operations & Abstract Data Structures*.

The Policy Machine's architecture was the basis for the NGAC work within INCITS. An initial standard from Project 2194-D was published in 2013 and is now available from the ANSI e-standards store as INCITS 499, *NGAC Functional Architecture (NGAC-FA)*. The standard resulting from Project 2195-D: INCITS 526, *NGAC Generic Operations and Abstract Data Structures (NGAC-GOADS)*, is in the approval process and is expected to be published in the fall of 2015.

In FY 2016, CSD plans to issue a new version of its open-source distribution to reflect new features and enhanced performance, revise INCITS 499, and publish SP 800-178, *A Comparison of Extensible Access Control Markup Language (XACML) and NGAC Attribute Based Access Control Standards for Data Services*.

## For More Information:

<http://csrc.nist.gov/pm/>

## CONTACTS:

Mr. David Ferraiolo  
(301) 975-3046  
[david.ferraiolo@nist.gov](mailto:david.ferraiolo@nist.gov)

Mr. Serban Gavrila  
(301) 975-4242  
[serban.gavrila@nist.gov](mailto:serban.gavrila@nist.gov)

## Security for a Virtualized Infrastructure

Several important components of a virtualized infrastructure need to be protected, including the Hypervisor, the virtual network, the Virtual Machine (VM) and data storage. The objective of this project is to analyze various configuration options in the deployment of these components and to provide guidance in the form of security recommendations. The project builds upon previous research that included: (a) the identification of security requirements for various use cases when a virtualized infrastructure is offered for cloud services and (b) the analysis of configuration options for Secure Hypervisor Deployment and providing security recommendations.

In FY 2015, the focus of research was the secure configuration of virtual networks for the protection of VMs. VM Security forms the primary goal in virtual network configuration due to the following: (a) VMs are the compute-engines of the virtualized infrastructure on which mission critical applications of the enterprise run, and (b) VMs are the end-nodes of the virtual network. Research included the following configuration areas:

- Network segmentation;
- Network path redundancy;
- Firewall deployment architecture; and
- VM traffic monitoring.

Research included the analysis of the security advantages and disadvantages of various configuration options in each of these areas, forming the basis for security recommendations. The research resulted in the following publications during FY 2015:

- The conference paper entitled, *Analysis of Network Segmentation Techniques in Cloud Data Centers*; and
- Draft SP 800-125B, *Secure Virtual Network Configuration for Virtual Machine (VM) Protection*.

## CONTACT:

Dr. Ramaswamy Chandramouli  
(301) 975-5013  
[mouli@nist.gov](mailto:mouli@nist.gov)

## Cybersecurity for Emerging Technologies

Technology is advancing at an amazing rate, with rapid technological advances in manufacturing, healthcare, nanotechnology, cyber physical systems, and the “Internet of things.” This project scans the environment for developing technologies that may be currently at risk from a cybersecurity perspective, or potentially at risk in the future as the technology improves.

In FY 2015, CSD conducted research on cybersecurity in the field of additive manufacturing or three-dimensional (3D) printing. On February 3, 2015, CSD hosted a symposium on *Cybersecurity for Direct Digital Manufacturing*, which involves fabricating physical objects from a data file using computer-controlled processes with little to no human intervention, such as in additive manufacturing and 3D printing. During the symposium, attendees representing government, industry, and academic organizations discussed relevant cybersecurity risks, challenges, and solutions, as well as the implications for information and communications technology supply-chain risk management. Attendees identified several opportunities in the area and generally agreed that the time is right for building cybersecurity into these technologies. The proceedings of the symposium were published in April 2015 in NISTIR 8041, *Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium*.

Along the same lines, CSD researched risk management practices for securing a set of technologies called Replication Devices (RDs). As a result of this research, CSD published NISTIR 8023, *Risk Management for Replication Devices*, in April 2015 to help organizations protect the confidentiality, integrity, and availability of information processed, stored, or transmitted on RDs. An RD is any device that reproduces (e.g., copies, prints, or scans) documents, images, or objects from an electronic or physical source. For the purposes of NISTIR 8023, RDs include copiers, printers, 3D printers, scanners, and 3D scanners, as well as multifunction machines when used as a copier, printer, or scanner. RDs in use within organizations run the gamut in terms of age and functionality, with some devices being relatively simple and others quite complex and sophisticated.



In FY 2016, NIST will continue to scan the environment for emerging technologies, such as 3D printers and nanotechnology, which may benefit from guidance on how to manage, implement, or build-in cybersecurity principles and tools.

---

## CONTACT:

Ms. Celia Paulsen  
(301) 975-5981  
celia.paulsen@nist.gov

## Cyber Threat Information Sharing

As cyber attacks increase in both sophistication and frequency, it is important to collect and analyze cyber threat information from a variety of internal and external sources, and use it to develop, enhance, and deploy proactive, threat-informed, cyber defense capabilities. Cyber threat information includes indicators (i.e., artifacts or observable events that suggest that an attack is imminent, that an attack is underway, or that a compromise may have already occurred); information about the tactics, techniques, and procedures (TTPs) of actors; recommended courses of action, and other information that is used to characterize threats. Because threat actors often use the same TTPs against multiple targets, exchanging cyber threat information allows organizations to leverage the collective knowledge, experience, and analysis capabilities of their peers, thereby increasing the overall awareness and security of an entire sharing community. Through the exchange of cyber threat information, organizations can gain a more complete understanding of their threat environment by correlating their observations with those of others.

When one organization observes an attack that may affect or be used against other organizations, information sharing and coordination can make it possible to reduce the impact of the attack, speed recovery operations, and maintain a higher level of operational security. By integrating cyber threat information sharing into its existing cybersecurity and risk management practices, an organization can reduce the likelihood or mitigate the impact of successful cyber attacks, more effectively protect its systems, detect and anticipate the actions of threat actors, respond to cyber attacks, and recover to rapidly deploy effective countermeasures.

In FY 2014, CSD worked with DHS to develop SP 800-150, *Guide to Cyber Threat Information Sharing (Draft)*, which provides guidance to organizations seeking to establish and participate in cyber threat information sharing communities. The draft publication was released for public comment on October 28, 2014. The goal of this publication

is to help organizations prepare for an exchange of cyber threat information, both consuming cyber threat information from external sources and producing information for other organizations to use. Because each organization may have substantially different capabilities for detecting threats, responding to attacks, diagnosing causes, and handling sensitive incident-related information, this guidance is intended to help organizations collaborate and exchange cyber threat information despite these organizational differences.

CSD's cyber threat information sharing initiative is focused on providing guidance on how an organization can establish information sharing and coordination capabilities that enhance or augment their existing cybersecurity practices. The guidance covers threat-informed detection, protection and response capabilities; data privacy and sensitivity; data collection and retention practices; the use of open standards for information exchange; de-identification and anonymization; and guidance on how an organization can establish, participate in, and maintain coordination and information sharing relationships. The guidance will help incident responders, network defenders, and operations personnel consider what information is sharable, the circumstances under which sharing is permitted, with whom the information may be shared, and how the information should be protected.

In early FY 2016, CSD plans to release the second draft to Draft SP 800-150, based on the input received during the public comment period of the first draft, which was released October 2014.

---

## CONTACTS:

Mr. Lee Badger  
(301) 975-3176  
lee.badger@nist.gov

Mr. David Waltermire  
(301) 975-3390  
david.waltermire@nist.gov

Mr. Christopher Johnson  
(301) 975-3247  
christopher.johnson@nist.gov

## The Ontology of Authentication

Over the past 30 years, NIST has been at the forefront of recommending best practices for authentication. Recommendations have included the usage of passwords in enterprises, biometrics, and Public Key Infrastructure (PKI) solutions. In FY 2015, CSD researched the classification of general authentication features. This investigation was prompted by the general call to move away from passwords towards the growing number of alternative authentication methods (e.g. biometrics, smart cards, etc.). In the early part of this investigation, it became clear that an ontology of authentication was needed.

A draft taxonomy (see Figure 19) was developed to better describe current and emerging authentication mechanisms. This taxonomy covers a wide assortment of commonly used methods to cover human-machine, machine-machine, and attribute attestation. It does not address identity management - which typically happens before authentication occurs, or access control - which typically happens after.

As a result of this research, several patterns and gaps were identified. For example, there are similar technologies used to support the various mechanisms. One of the greatest challenges is in defining a set of common metrics to assess authentication technologies. Two areas identified as needing

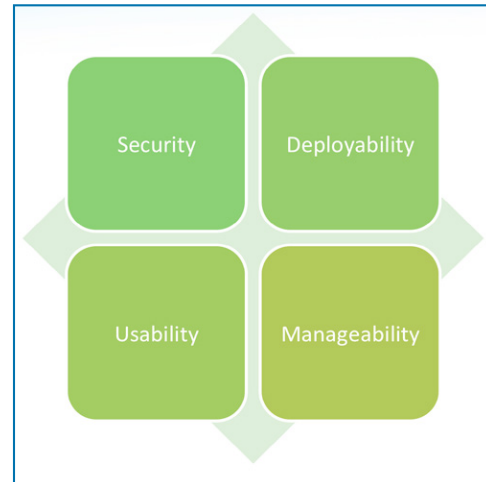


Figure 20: Suitability Framework for Authentication

metrics include authentication strength and the suitability of the method to the environment. The strength measurements should include security and usability. This provides a way to monitor a common complaint of designers – usability being a tradeoff to security. However, security and usability is not sufficient to address the suitability of implementing a particular authentication mechanism in a particular environment. By adding in measures for deployability and manageability it should be possible to address the suitability of an authentication mechanism.

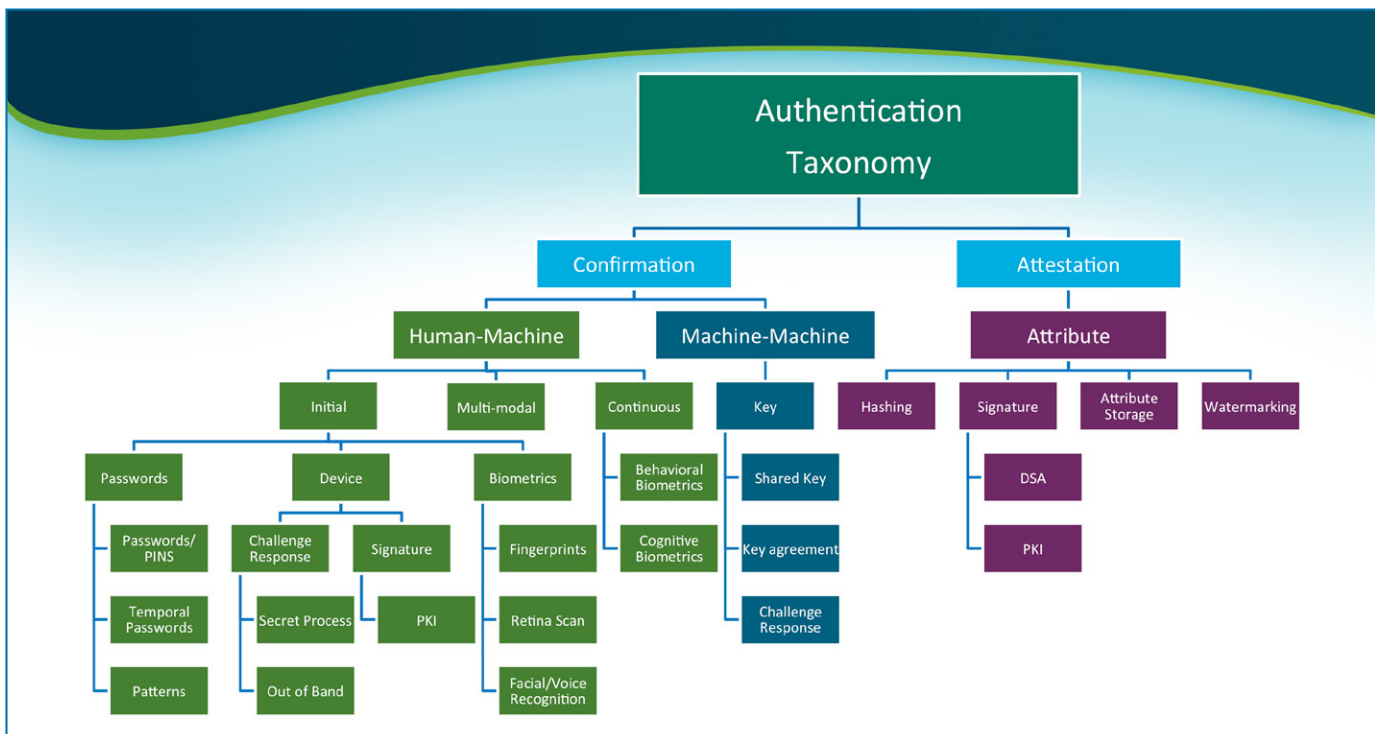


Figure 19: Draft Authentication Taxonomy

In the next few years, NIST CSD will work with the community to identify and address common areas of authentication requirements to create a framework for researching and developing authentication mechanisms using this taxonomy. As shown in Figure 20 (previous page), this framework will support integration of security with deployability, usability and manageability of authentication. This work will also be used to better identify the needs and dependencies for proper interaction with identity management and access control processes.

## CONTACT:

Dr. Kim Schaffer  
(301) 975-8375  
kim.schaffer@nist.gov

NIST's work in mobile security has earned the 2014 Government Computer News (GCN) award for Information Technology Excellence and the 2013 U.S. Department of Commerce Gold Medal Award. In FY 2016, NIST will be transitioning AppVet to the Department of Homeland Security as part of their Carwash program, which provides government development teams with a continuous integration build, testing, source code management, and issue tracking system.

## CONTACTS:

Dr. Steve Quirolgico  
(301) 975-8426  
steveq@nist.gov

Dr. Jeffrey Voas  
(301) 975-6622  
jeff.voas@nist.gov

## MOBILE SECURITY

Smart phones have become both ubiquitous and indispensable. Although these mobile devices are relatively small and inexpensive, they can be used for voice calls, simple text messages, sending and receiving emails, browsing the web, online banking and e-commerce, social networking, and many functions once limited to laptop and desktop computers. Smart phones and tablet devices have specialized built-in hardware, such as cameras, accelerometers, Global Positioning System (GPS) receivers, and removable media readers. They also employ a wide range of wireless interfaces, including infrared, Wireless Fidelity (Wi-Fi), Bluetooth, Near Field Communications (NFC), and one or more types of cellular interfaces that provide network connectivity across the globe.

Smart phones present new capabilities, but also a number of new security and privacy challenges. One such challenge concerns securing smartphone applications. To address this issue, NIST is conducting research in software-assurance methodologies for smart phone applications (or "apps") and is working with other government agencies and industry to bridge the security gaps present with today's smart phones. For example, NIST developed the AppVet mobile app-vetting system and framework for managing an organization's app-vetting process with respect to the organization's security and privacy policies. This system was used by the Defense Advanced Research Projects Agency (DARPA) to vet apps prior to being deployed on thousands of mobile devices for use in Afghanistan, the 2013 Presidential Inauguration, and the 2014 Boston Marathon.

## STRENGTHENING INTERNET SECURITY

### USGv6: A Technical Infrastructure to Assist IPv6 Adoption

Internet Protocol (IP) Version 6 (IPv6) is an updated version of the current Internet Protocol, IPv4. The primary motivations for the development of IPv6 were to increase the number of unique IP addresses available for use and to handle the needs of new Internet applications and devices. In addition, IPv6 was designed with the following goals: increased ease of network management and configuration, expandable IP headers, improved mobility and security, and the quality of service controls. IPv6 has been, and continues to be, developed and defined by the IETF.

FY 2012 was a significant year for the deployment of IPv6 in the United States Government (USG). OMB's Memo of September 10, 2010, *Transition to IPv6*, required all government agencies to "upgrade public/external facing servers and services (e.g., web, email, Domain Name System (DNS), and Internet Service Provider (ISP) services) to operationally use IPv6 by the end of FY 2012." NIST worked with the U.S. Government IPv6 (USGv6) Task Force and with individual government agencies to achieve this goal. NIST developed an online monitor to demonstrate which high-level government domains have met this goal with respect to Domain Name System (DNS) services, email, web servers, and Domain Name System Security Extensions (DNSSEC). In FY 2013, NIST and OMB continued to use this monitor to measure USGv6 compliance with OMB's requirement.

Additional OMB IPv6 requirements were mandated for FY 2014. Agencies were required to “upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use IPv6 by the end of FY 2014.” NIST developed online diagnostic tools to help agencies verify compliance to this requirement.

The NIST IPv6 Test Program, whose goal is to provide assurance on IPv6 product conformance and interoperability, continues to operate. In FY 2015, NIST continued to manage and evolve the USGv6 Test Program and to help federal agencies fulfill OMB mandates and monitor compliance to those mandates. In FY 2016, NIST is planning to update SP 500-267, *A Profile for IPv6 in the U.S. Government, Version 1.0*. This document is the basis for the USGv6 Test Program and for USG IPv6-compliant device evaluation and purchase. The NIST program is a collaboration between CSD and the ITL Advanced Networking Technology Division.

#### For More Information, See:

<http://www.nist.gov/itl/antd/usgv6.cfm>

### CONTACTS:

Ms. Sheila Frankel  
(301) 975-3297

[sheila.frankel@nist.gov](mailto:sheila.frankel@nist.gov)

Mr. Douglas Montgomery  
(301) 975-3630

[doug.m@nist.gov](mailto:doug.m@nist.gov)

- Published a conference paper for Big Data Processing access control and distributed systems; and
- Studied efficient test case generation methods for Attribute Based Access Control (ABAC) policy testing.

In FY 2016, CSD will continue the above research. CSD expects that this project will:

- Promote (or accelerate) the adoption of community computing that utilizes the power of shared resources and common trust-management schemes;
- Provide guidance for implementing access control models and mechanisms for standalone or network systems;
- Increase the security and safety of static (connected) distributed systems by applying the testing and verification tool for the AC policies;
- Assist system architects, security administrators, and security managers whose expertise is related to access control or privilege policy in managing their systems and in learning the limitations and practical approaches for their applications; and
- Provide accurate and efficient fault detection and correction technology for implementing AC rules and policies.

Figure 21 illustrates the application of access control and privilege management within and among organizations.

## ACCESS CONTROL PROJECTS

### Access Control and Privilege Management Research

With the advance of current computing technologies and the diverse environments, access control issues, such as situational awareness, trust management, preservation of privacy, and privilege-management systems, are becoming increasingly complex. Practical and conceptual guidance for these topics is needed.

In FY 2015, the following research was accomplished for this project:

- Enhanced the unified enforcement mechanism of data services for use by a Policy Machine (PM) for an enterprise computing environment;
- Enhanced the capabilities of the Access Control Policy Tool (ACPT);
- Enhanced the capabilities of the Access Control Rule Logic Circuit Simulation (ACRLC) tool;
- Studied an Attribute Assurance mechanism for access authentication and authorization;

64

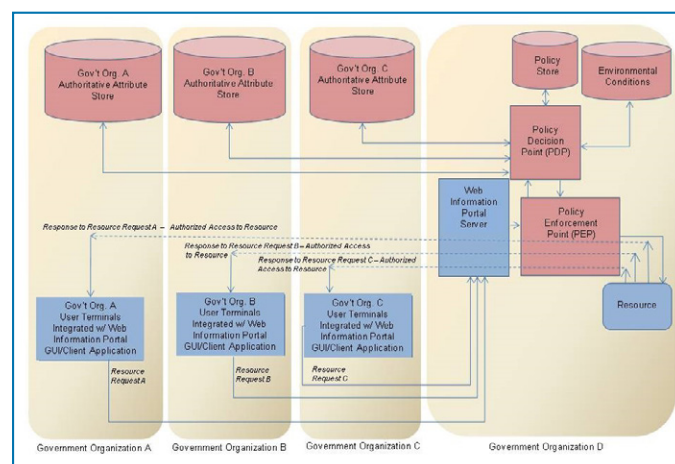


Figure 21: Access Control and Privilege Management

### CONTACTS:

Dr. Vincent Hu  
(301) 975-4975  
[vhu@nist.gov](mailto:vhu@nist.gov)

Mr. Rick Kuhn  
(301) 975-3337  
[kuhn@nist.gov](mailto:kuhn@nist.gov)

Mr. David Ferraiolo  
(301) 975-3046  
[david.ferraiolo@nist.gov](mailto:david.ferraiolo@nist.gov)



## Conformance Verification for Access Control Policies

Access control (AC) systems are among the most critical network security components. Faulty policies, misconfigurations, or flaws in software implementation can result in serious vulnerabilities. The specification of access control policies is often a challenging problem. Often, a system's privacy and security are compromised due to the misconfiguration of access control policies, instead of the failure of cryptographic primitives or protocols. This problem becomes increasingly severe as software systems become more and more complex, and are deployed to manage a large amount of sensitive information and resources organized into sophisticated structures. Identifying discrepancies between policy specifications and their properties (their intended function) is crucial because correct implementation and enforcement of policies by applications is based on the premise that the policy specifications are correct. As a result, policy specifications must undergo rigorous verification and validation through systematic testing to ensure that the policy specifications truly encapsulate the desires of the policy authors.

To formally and precisely capture the security properties that AC should adhere to, access control models are usually written to bridge the rather wide gap in abstraction between policy and mechanism. Thus, an access-control model provides unambiguous and precise expression, as well as a reference for the design and implementation of security requirements. Techniques are required for verifying whether an access-control model is correctly expressed in the access-control policies, and whether the properties are satisfied in the model.

Most research on AC model or policy verification techniques is focused on one particular model, and almost all of the research is in applied methods, which require the completed AC policies as the input for verification or test processes to generate fault reports. Even though correct verification is achieved, and counter-examples may be generated when faults were found, those methods provide no information about the source of faults that might allow conflicts in privilege assignment, the leakage of privileges, or conflict of interest permissions. The difficulty in finding the source of faults is increased, especially when the AC rules are intricately covering duplicated variables to a degree of complexity. The complexity is due to the fact that a fault might not be caused by one particular rule. Thus, it requires manually analyzing each rule in the policy in order to find the correct solution for the fault.

To address the issue, CSD developed the Access Control Property Tool (ACPT), shown in Figure 22 (next page), which allows a user to compose, verify, test, and generate access control policies. CSD also researched the AC Rule Logic Circuit Simulation (ACRLCS) technique, which enables the AC authors to detect a fault when the fault-causing AC rule is added to the policy, so the fix can be implemented in real time before adding other rules that further complicate the detecting effort, rather than checking by retracing the interrelations between rules after the policy is completed.

In FY 2015, CSD accomplished the following:

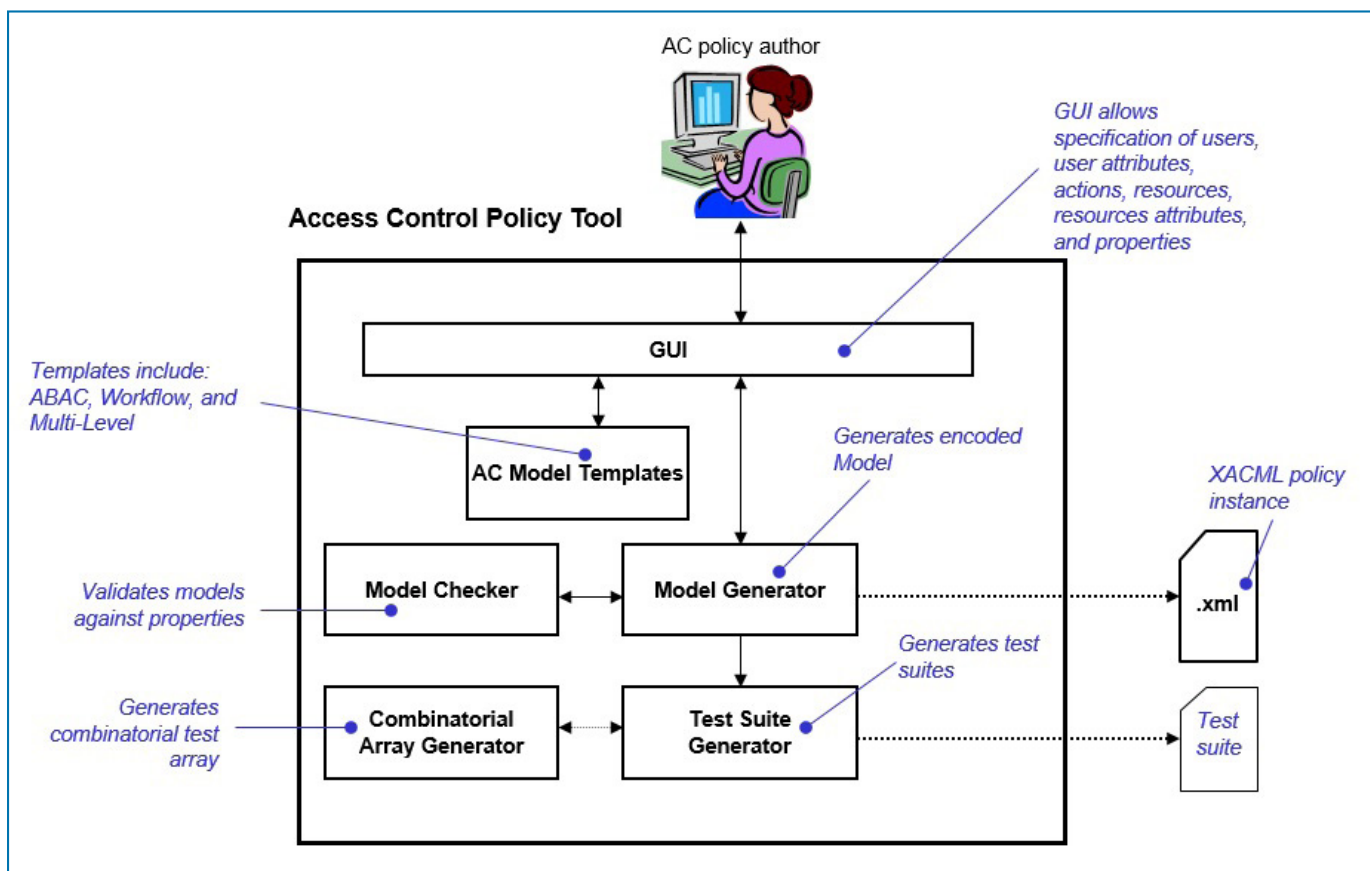
- Published a conference paper for policy tool evaluation and analysis: *Evaluating and Capability and Performance of Access Control Policy Verification Tools*;
- Developed verification oracles for policy test benchmarking, which embed policy faults for committee, university, hospital, and bank policy test scenarios;
- Developed a Small Business Innovation Research (SBIR) solicitation for access control tool development;
- Enhanced the ACRLCS – the Access Control Rule Logic Circuit Simulation System;
- Published a conference paper for policy test case generation: *Pseudo-exhaustive Testing of Attribute-Based Access Control Rules*;
- Worked with industrial and academic organizations in exploring new capabilities that helped to improve the usability of the AC tools (ACPT and ACRLCS), resulting in additional usage; ACPT was downloaded by 343 users and organizations; and,
- Enhanced the capability of ACPT by improving policy combination algorithms and adding test oracles for basic access control models.

In FY 2016, CSD is planning to conduct further research on the new capabilities and enhance the performance of the ACPT and ACRLCS.

Figure 22 (next page) shows the system architecture of the NIST access control policy tool: ACPT, which allows access control policy authors to compose, verify, and test access control policy implementation.

This project is expected to:

- Provide a generic paradigm and framework of access control model/property conformance testing;
- Provide templates for specifying access control rules in popular access control models, such as the Attribute Based, Multilevel, and Workflow models;



**Figure 22: Access Control Property Tool (ACPT)**

- Provide tools or services for checking the security and safety of an access control implementation, policy combination, and eXtensible Access Control Markup Language (XACML) policy generation;
- Promote (or accelerate) the adoption of combinatorial testing for large-system testing (such as an access control system);
- Promote the concept of detecting AC policy faults in real-time AC rule composing;
- Provide an innovative method for specifying AC rules formed by Boolean logic expressions operated on variables of AC rules;
- Provide techniques for preventing faults in enforcing fundamental security properties, including Cyclic Inheritance, Privilege Escalation, and Separation of Duty; and
- Provide new methods for composing standard mandatory AC models, such as Attribute-Based Access Control (ABAC) and Multi-Level Security (MLS), as well as some fundamental security properties.

#### For More Information, See:

<http://csrc.nist.gov/groups/SNS/acpt/>

#### CONTACTS:

Dr. Vincent Hu  
(301) 975-4975  
vhu@nist.gov

Mr. Rick Kuhn  
(301) 975-3337  
kuhn@nist.gov

#### Attribute-Based Access Control

Attribute-Based Access Control (ABAC) is a logical access control methodology where an authorization to perform a set of operations is determined by evaluating the attributes associated with the subject, object, requested operations, and, in some cases, environmental conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes. ABAC represents a point on the spectrum of logical access control, from simple access control lists to more capable role-based access (RBAC), and finally, to a highly flexible method for providing access based on the evaluation of attributes.

This research provides information for using ABAC to improve information sharing within and among organizations based on the planning, design, implementation, and operational considerations. The research also includes technologies such as attribute assurance, attribute engineering/management, identity system integration, attribute federation, situational awareness (real-time or contextual) mechanisms, policy management, and natural-language policy translation to digital policy. Figure 23 illustrates the interaction of many of these components. The goal of this research is to improve information sharing, while maintaining control of that information for federal agencies.

In FY 2015, CSD published two ABAC papers: *Attribute-Based Access Control* for *IEEE Computing* magazine, and *Implementing and Managing Policy Rules in Attribute-Based Access Control* for *IEEE International Conference on Information Reuse and Integration*. CSD also wrote a draft Special Publication document for ABAC formal models research: *A Comparison of XACML and NGAC Attribute Based Access Control Standards*, which compares the

characteristics of two ABAC implementation mechanisms: XACML and NGAC. CSD continued research on the Attribute Assurance of ABAC in partnership with the National Strategy for Trusted Identities in Cyberspace (NSTIC), and the National Cybersecurity Center of Excellence (NCCoE). CSD developed a draft Special Publication based on the mechanism for defining the veracity, security, and readiness levels of assurance of ABAC attributes.

In FY 2016, CSD will continue the research of ABAC formal models, as well as details and extended topics of ABAC capabilities, such as attribute assurance, ABAC implementation examples, ABAC mechanisms, and ABAC standards. The ABAC project will pursue the following objectives:

- Provide readers with the terminology and a basic understanding of ABAC;
- Provide readers with an overview of the current state of logical access control, a working definition of ABAC, and an explanation of the core and enterprise ABAC concepts;

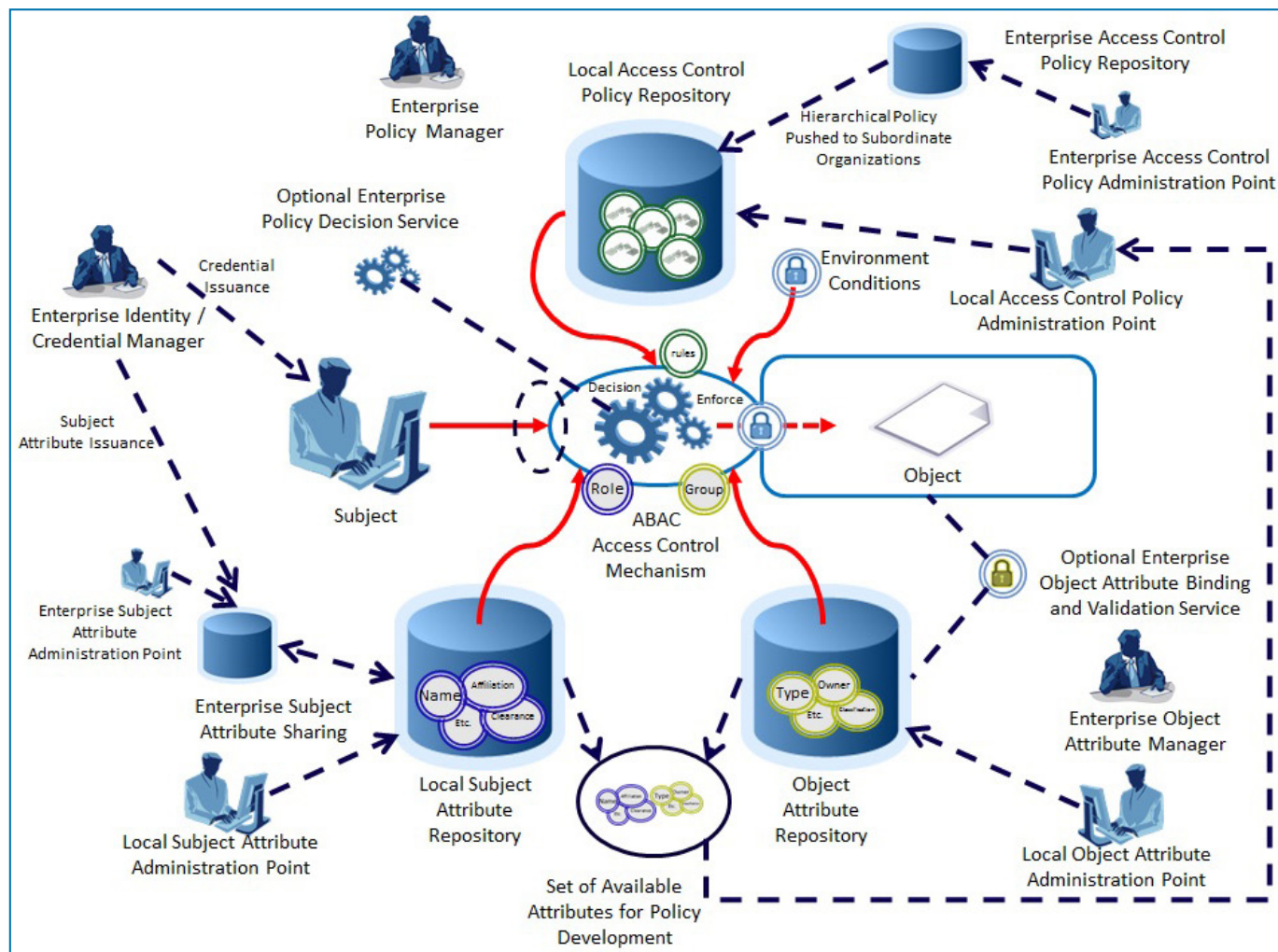


Figure 23: ABAC Access Control Mechanism Chart



- Assist security policy makers in establishing a business case for ABAC implementation and acquiring an interoperable set of capabilities;
- Assist ABAC developers in developing the operational requirements and overall enterprise architecture;
- Assist ABAC administrators in establishing or refining business processes to support ABAC;
- Promote the adoption of ABAC for a more secure and flexible method for information sharing in a standalone or enterprise environment; and
- Provide testing methods for ABAC policy and implementations.

#### For More Information, See:

<http://csrc.nist.gov/projects/abac/>

### CONTACTS:

Dr. Vincent Hu  
(301) 975-4975  
vhu@nist.gov

Mr. David Ferraiolo  
(301) 975-3046  
david.ferraiolo@nist.gov

Mr. Rick Kuhn  
(301) 975-3337  
kuhn@nist.gov

## ADVANCED SECURITY TESTING AND MEASUREMENTS

### Security Automation and Continuous Monitoring

IT organizations operate a diverse set of computing assets that access, route, store, and process information that is critical to the operations of businesses and the missions of government agencies. These IT environments are under constant threat of attack and are frequently undergoing change, with new and updated software being deployed along with updated configurations. The wide variety of computing products, the dynamic nature of software, the speed of configuration change, and the diversity of threats require organizations to maintain situational awareness over their IT assets and to utilize this information to make informed risk-based decisions.

Security automation utilizes standardized data formats and transport protocols to enable data to be exchanged between business, operational, and security systems that support security processes by:

- Identifying IT assets, including hardware, software, and data;
- Providing awareness over the operational state of computing devices;
- Enabling security reference data to be collected from internal and external sources; and
- Supporting analysis processes that measure the effectiveness of security controls and provide visibility into security risks, enabling risk-based decision-making.

Commercial solutions built using security automation specifications enable the collection and harmonization of vast amounts of operational and security data into coherent, comparable information streams to achieve situational awareness that allows the timely and active management of diverse IT systems. Through the creation of reference data and guidance, and the international recognition of flexible, open standards, the NIST security automation program works to improve the interoperability, broad acceptance, and adoption of security automation solutions to address current and future security challenges, creating opportunities for innovation.

### Specification, Standards, and Guidance Development

To support the overarching security automation vision, it is necessary to have specifications that describe the required interactions between systems, standards that document international consensus approaches, and guidance that informs product developers and implementers. Through close work with partners in government, industry, and academia, CSD continues to facilitate the definition and development of security automation approaches that enable organizations to understand and manage IT security risks.

During FY 2015, CSD has continued to work to build on previous security automation work by:

- Identifying and addressing gaps in the current specifications;
- Evolving existing approaches to achieve greater scalability and impact;
- Participating in working groups in standards development organizations to promote international consensus around standardized approaches;
- Providing additional guidance on architectural, design, and analysis concerns; and
- Developing and maintaining tools and reference implementations.



CSD is currently working with its partners in various standards-development organizations, including ISO, IETF, the Forum of Incident Response and Security Teams (FIRST), and the Trusted Computing Group (TCG), to further mature and broaden the adoption of security automation specifications, reference data, and techniques. This area of work is focused on evolving security automation specifications to integrate with existing transport protocols to provide for the secure, interoperable exchange of security automation data. Additional work is focused on evolving security metrics and providing consensus guidance on security automation approaches. Through the definition and adoption of security automation standards and guidelines, IT vendors will be able to provide standardized security solutions to their customers. These solutions support continuous monitoring and automated, dynamic network defense capabilities, based on the analysis of data from operational and security data sources and the collective action of security components.

Security automation standardization work has been focused in three areas: the evolution and international adoption of the Security Content Automation Protocol (SCAP), the development of software asset management standards to support operational and cybersecurity use cases, and the development of security automation consensus standards. The following sections detail this work.

## Security Content Automation Protocol (SCAP)

SCAP is a multipurpose protocol that provides an automated means to collect and assess the state of devices. SCAP supports automated vulnerability checking, verifying the installation of patches, checking security configuration settings, verifying technical-control compliance, measuring security, and examining systems for indicators of a compromise. SCAP uses the Extensible Markup Language (XML) to standardize the format and nomenclature by which security software products communicate information about software flaws, security configurations, and other aspects of the device state. SCAP enables security automation content, also known as “SCAP content,” to be expressed using standardized formats, identifiers, and scoring models. This content can be used by any tool that is conformant to the specifications to collect and evaluate the state of software installed on a device.

SCAP has been widely adopted by major software and hardware manufacturers and has become a significant component of information-security-management and governance programs. SCAP-enabled tools are currently being used by the U.S. Government, critical-infrastructure companies, academia, and other businesses, both domestically and internationally. Currently, CSD is leveraging

SCAP in multiple areas, both to support its own mission and to enable other agencies and private-sector entities to meet their goals. For CSD, SCAP is a critical component of the SCAP Validation Program, the National Vulnerability Database (NVD), and the National Checklist Program (NCP).

In September 2012, CSD published SP 800-126 Rev. 2, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*. That document describes the 11 component specifications composing SCAP. See Table 2 (next page): SCAP 1.2 Specifications for details.

Since the release of SCAP 1.2, CSD has worked to improve guidance around the use of SCAP specifications. In FY 2015, CSD released draft NISTIR 8058, *Security Content Automation Protocol (SCAP) Version 1.2 Content Style Guide: Best Practices for Creating and Maintaining SCAP 1.2 Content*, which provides guidance for SCAP 1.2 content creators to ensure that stylistic variations in SCAP 1.2 content are addressed in a way that improves the accuracy and consistency of results, avoids performance problems, reduces user effort, lowers content maintenance burdens, and enables content reuse. To achieve this, the report documents best practices for content creation and encourages their use by SCAP content authors and maintainers. Feedback on this report is welcomed and will help CSD to work towards producing a final version of this document.

CSD is starting to work on an SCAP 1.3 revision. In August 2015, CSD requested comments on the design and development of SCAP 1.3. Specific areas of requested feedback included:

- Adopting the Open Vulnerability and Assessment Language (OVAL) 5.11.1, which was released in April 2015;
- Adopting the Common Vulnerability Scoring System (CVSS) v3, which was released in June 2015;
- Removing support for CVSS v2; and
- Deprecating support for older specification revisions and SCAP 1.0.

The received feedback generally favored the adoption of OVAL 5.11.1 and CVSS v3. Continued support for CVSS v2, in addition to v3, and some reduction in the minimal support for older specification revisions were also common themes in the feedback. CSD is currently considering this feedback while working on a draft revision of SP 800-126 for public comment in FY 2016.

**TABLE 2: SCAP 1.2 SPECIFICATIONS**

SPECIFICATIONS	DESCRIPTION
<b>Languages</b>	
Extensible Configuration Checklist Description Format (XCCDF)	Used for authoring security checklists/benchmarks and for reporting results of evaluating them
Open Vulnerability and Assessment Language (OVAL)	Used for representing system-configuration information, assessing machine state, and reporting assessment results
Open Checklist Interactive Language (OCIL)	Used for representing checks that collect information from people or from existing data stores populated by other data collection methods
<b>Reporting Formats</b>	
Asset Reporting Format (ARF)	Used to express information about assets and to define the relationships between assets and reports
Asset identification	Used to uniquely identify assets based on known identifiers and other asset information
<b>Enumerations</b>	
Common Platform Enumeration (CPE)	A nomenclature and dictionary of hardware, operating systems, and applications; a method to identify applicability to platforms
Common Configuration Enumeration (CCE)	A nomenclature and dictionary of software-security configurations
Common Vulnerabilities and Exposures (CVE)	A nomenclature and dictionary of security-related software flaws
<b>Measurement and Scoring Systems</b>	
Common Vulnerability Scoring System (CVSS)	Used for measuring the relative severity of software flaws
Common Configuration Scoring System (CCSS)	Used for measuring the relative severity of device security (mis-)configuration issues
<b>Content and Result Integrity</b>	
Trust Model for Security Automation Data (TMSAD)	Guidance for using digital signatures in a common trust model applied to security automation specifications

## Software Asset Management Standards

CSD has been collaborating with industry partners to revise the ISO/IEC 19770-2:2009 standard, *Information technology—Software asset management—Part 2: Software identification tag*, which establishes a specification for tagging software to support identification and management. An updated revision of this standard, ISO/IEC 19770-2:2015, was published on October 1, 2015. The software identification (SWID) data model defined by this standard describes an XML format for software publishers to provide authoritative identification, categorization, software relationships (e.g., dependency, bundling, and patch), executable and library footprint details, and other metadata for software. This information can be used to support operational and cybersecurity use cases around managing software deployments, managing software licenses, managing software vulnerabilities and related software patches, and assessing secure software configurations.

To supplement the requirements in ISO/IEC 19770-2:2015, CSD has been working with DHS and NSA on the development of NISTIR 8060, *Guidelines for the Creation of Interoperable Software Identification (SWID) Tags*. NISTIR 8060 provides an overview of the capabilities and usage of software identification (SWID) tags as part of a comprehensive software lifecycle. This report introduces SWID tags in an operational context, provides guidelines for the creation of interoperable SWID tags, and highlights key usage scenarios for which SWID tags are applicable. Figure 24 illustrates how SWID tags support multiple elements of the software product life cycle, including deployment,

installation, patching, upgrading and removal. CSD has released three public discussion drafts of these guidelines. A final public draft will be released in FY 2016, along with a subsequent final release of the report.

Additionally, NIST has worked with the TCG to integrate SWID tags into the Trusted Network Communications (TNC) protocol, through the SCAP Messages for IF-M specification that will be discussed below.

The information provided within SWID tags enhances the SCAP use cases by providing authoritative information that can be used to create Common Platform Enumeration (CPE) names, to support the targeting of checklists, and to associate software flaws to products, based on a defect in a software library or executable. CSD will be working on a number of reports in FY 2016 that provide further guidance for using SWID tags to address these use cases.

## Development of Security Automation Consensus Standards

CSD has been promoting the broad international adoption of SCAP by encouraging the integration of SCAP into other standards, and by adapting SCAP to address specific gaps and challenges. CSD has continued its collaboration with industry partners in the IETF Security Automation and Continuous Monitoring (SACM) working group. This working group provides a venue for advancing appropriate SCAP specifications into international standards and addressing identified gap areas. The current scope of work for SACM includes identifying and/or defining the transport protocols and data formats needed to support

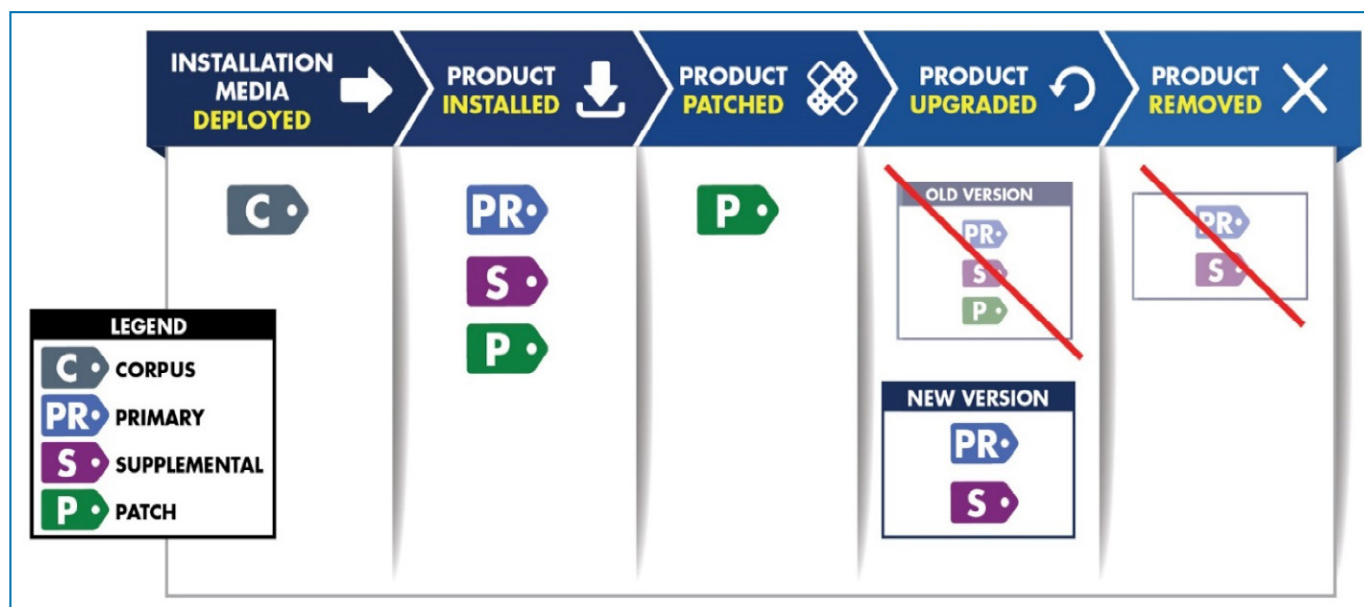


Figure 24: SWID Tags Support the Software Product Lifecycle

the collection and evaluation of a device state against expected values. Over the past twelve months, the SACM working group has been working on identifying use cases, requirements, and architectural models to inform decisions about existing specifications and standards that can be referenced, required modifications or extensions to existing specifications and standards, and any gaps that need to be addressed. CSD is working with DHS, the Center for

Internet Security (CIS), and the TCG to bring existing work into the IETF SACM working group to include OVAL and specifications related to the TNC protocol.

In FY 2015, the SACM use cases were published by the IETF as Request for Comments (RFC) 7632.

The working group has been developing the following Internet Drafts:

INTERNET DRAFT	PURPOSE
<a href="https://datatracker.ietf.org/doc/draft-ietf-sacm-terminology/">https://datatracker.ietf.org/doc/draft-ietf-sacm-terminology/</a>	Definition of the common terminology used within a number of working-group documents.
<a href="https://datatracker.ietf.org/doc/draft-ietf-sacm-requirements/">https://datatracker.ietf.org/doc/draft-ietf-sacm-requirements/</a>	Listing architectural and specification requirements for SACM specifications.
<a href="https://datatracker.ietf.org/doc/draft-ietf-sacm-architecture/">https://datatracker.ietf.org/doc/draft-ietf-sacm-architecture/</a>	Definition of the SACM architecture to inform development of transports.
<a href="https://datatracker.ietf.org/doc/draft-ietf-sacm-information-model/">https://datatracker.ietf.org/doc/draft-ietf-sacm-information-model/</a>	Definition of the SACM information model to inform development of data models.

For more information, please refer to: <http://datatracker.ietf.org/wg/sacm/charter/>

CSD also worked with government and industry partners in the TCG to define a number of specifications related to the TNC protocol. The first such publication is the TNC SCAP Messages for IF-M specification that supports carrying SCAP content and results over the TNC protocols. The second is the TNC Enterprise Compliance Profile (ECP) and related specifications that support the exchange of SWID data over the TNC protocols. The ECP enables the collection of SWID data from a device for use by external tools to provide software inventory information. SCAP and SWID data collected using these mechanisms may be optionally used for network access-control decision making, allowing the device state to be evaluated when devices connect and on an ongoing basis thereafter.

For more information on these specifications, please visit: [http://www.trustedcomputinggroup.org/resources/tnc\\_scap\\_messages\\_for\\_ifm](http://www.trustedcomputinggroup.org/resources/tnc_scap_messages_for_ifm), and [http://www.trustedcomputinggroup.org/resources/tnc\\_endpoint\\_compliance\\_profile\\_specification](http://www.trustedcomputinggroup.org/resources/tnc_endpoint_compliance_profile_specification).

Finally, CSD has worked with the FIRST by participating in two Special Interest Groups (SIGs). The CVSS SIG (CVSS-SIG) is focused on maintaining and improving the CVSS scoring model, based on community feedback. The CVSS-SIG published CVSS Revision 3 (CVSS v3) in June 2015. The second SIG, the Vulnerability Reporting and Data eXchange SIG (VRDX-SIG), researches and recommends methods for

identifying and exchanging vulnerability information across disparate vulnerability databases.

For more information, please visit: <http://www.first.org/global/sigs>.

Through work with international standards-developing organizations (SDOs), SCAP and related security automation capabilities are expected to evolve and expand in support of the growing need to define and measure effective security controls, assess and monitor ongoing aspects of information security, remediate noncompliance, and successfully manage systems in accordance with the Risk Management Framework described in SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. Standards that are developed and published by these SDOs will be considered for inclusion in future revisions of SCAP.

#### For More Information, See:

<http://scap.nist.gov/>

#### CONTACT:

Mr. David Waltermire  
(301) 975-3390  
[david.waltermire@nist.gov](mailto:david.waltermire@nist.gov)



## Security Automation Reference Data

Through the NVD and the NCP, NIST is providing relevant and important reference data in the areas of vulnerability and configuration management. SCAP and the programs that leverage it are moving the information assurance industry towards being able to standardize communications, and towards the collection and storage of relevant data in standardized formats, as well as providing automated means for the assessment and remediation of systems for both vulnerabilities and configuration compliance.

## National Vulnerability Database (NVD)

Security automation reference data is currently housed within the NVD. The NVD is the U.S. Government repository of security automation data based on security automation specifications. This data provides a standards-based foundation for the automation of software asset, vulnerability, and security configuration management; security measurement; and compliance activities. This data supports security automation efforts based on the SCAP. The NVD includes databases of security configuration checklists for the NCP, listings of publicly known software flaws, product names, and impact metrics. A formal validation program tests the ability of vendor products to use some forms of security automation data, based on a product's conformance in support of specific enterprise capabilities.

SCAP defines the structure of standardized software flaws and security configuration reference data, also known as SCAP content. This reference data is provided by the NVD (<http://nvd.nist.gov/>).

As of October 2015, the NVD contained the following resources:

- Over 72,000 vulnerability advisories, with an average of 40 new vulnerabilities added daily;
- 82 SCAP-expressed checklists containing thousands of low-level security configuration checks that can be used by SCAP-validated security products to perform automated evaluations of the system state;
- 248 non-SCAP security checklists (e.g., English prose guidance and configuration scripts);
- 249 U.S. Computer Emergency Readiness Team (US-CERT) alerts; 4,402 US-CERT vulnerability summaries; and 10,286 SCAP machine-readable software flaw checks; and;
- A product dictionary with over 106,000 operating system, application, and hardware name entries; and over 58,000 vulnerability advisories translated into Spanish.

NVD is hosted and maintained by NIST and is sponsored by the Department of Homeland Security's US-CERT.

The use of SCAP data by commercial security products, deployed in thousands of organizations worldwide, has extended NVD's effective reach. Increasing demand for NVD XML data feeds (i.e., mechanisms that provide updated data from data sources) and SCAP-expressed content from the NVD website demonstrates an increased adoption of SCAP.

The NVD continues to play a pivotal role in the Payment Card Industry (PCI) efforts to mitigate vulnerabilities in credit card systems. PCI mandates the use of NVD vulnerability severity scores in measuring the risk to payment card servers worldwide and for prioritizing vulnerability patching. PCI's use of NVD severity scores helps enhance credit card transaction security and protects consumers' personal information.

### For More Information, See:

<https://nvd.nist.gov>

## CONTACTS:

Mr. Harold Booth  
(301) 975-8441  
[harold.booth@nist.gov](mailto:harold.booth@nist.gov)

Mr. Robert Byers  
(301) 975-3279  
[robert.byers@nist.gov](mailto:robert.byers@nist.gov)

## National Checklist Program (NCP)

There are many threats to information technology (IT), ranging from remotely launched network service exploits to malicious code spread through infected emails, websites, and downloaded files. Vulnerabilities in IT products are discovered daily, and many ready-to-use exploitation techniques are widely available on the Internet. Because IT products are often intended for a wide variety of audiences, restrictive security configuration controls are usually not enabled by default. As a result, many out-of-the box IT products are immediately vulnerable. In addition, identifying a reasonable set of security settings that achieve balanced risk management is a complicated, arduous, and time-consuming task, even for experienced system administrators.

To facilitate the development of security configuration checklists for IT products and to make checklists more organized and usable, CSD established the National Check-list Program (NCP) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347, and also under the Cybersecurity Research and Development Act, which mandates that NIST "develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer

hardware or software system that is, or is likely to become, widely used within the Federal Government.” In February 2008, revised Part 39 of the Federal Acquisition Regulation (FAR) was published. Paragraph (d) of section 39.101 states, “In acquiring information technology, agencies shall include the appropriate IT security policies and requirements, including use of common security configurations available from the NIST website at <http://checklists.nist.gov>. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.”

In Memorandum M-08-22, OMB mandated the use of SCAP-validated products for the continuous monitoring of Federal Desktop Core Configuration (FDCC) compliance. The NCP strives to encourage and assist federal agencies with these mandates.

The goals of the NCP are to:

- Facilitate the development and sharing of checklists by providing a formal framework for checklist developers to submit checklists to NIST;
- Provide guidance to developers to help them create standardized, high-quality checklists that conform to common operation environments;
- Help developers and users by providing guidelines for making checklists better documented and more usable;
- Encourage software vendors and other parties to develop checklists;
- Provide a managed process for the review, update, and maintenance of checklists;
- Provide an easy-to-use repository of checklists; and
- Encourage the use of automation technologies (e.g., SCAP) for checklist application.

NCP added 100 new checklists in FY 2015, bringing the number of checklists posted on the website to 353 (see <http://checklists.nist.gov>). Of that total, 153 of the checklists, addressing 86 platforms, are SCAP-expressed and can be used with SCAP-validated products. This represents a 45 % increase in the number of SCAP-expressed checklists when compared to FY 2014, demonstrating continual use and adoption of this automated means of expressing and consuming checklist content.

Organizations can use checklists obtained from the NCP website for automated security configuration patch assessment. The NCP currently hosts SCAP checklists for Internet Explorer 9.0, Internet Explorer 10.0, Office 2010, Red Hat Enterprise Linux, Windows 7, Windows 8, Windows Server 2012, and other products.

To assist users in identifying automated checklist content, NCP groups these checklists into tiers, from Tier I to Tier IV. The NCP uses the tiers to rank checklists according to their automation capability. Tier III and IV checklists include fully vetted SCAP content that has successfully demonstrated conformance to the requirements outlined in SP 800-126. Tier III & IV checklists are considered production-ready and are intended for use with SCAP-validated products.

Tier II checklists document recommended security settings in a machine-readable, nonstandard format, such as a proprietary format or a product-specific configuration script. Tier I checklists are prose-based and contain no machine-readable content. Users can browse the checklists, based on the checklist tier, IT product, IT product category, or authority, and through a keyword search that searches the checklist name and summary for user specified terms. The search results show the detailed checklist metadata and a link to any SCAP content for the checklist, as well as links to any supporting resources associated with the checklist.

To assist checklist developers, the NCP provides both manual and automated interfaces to facilitate the submission and maintenance processes. The manual interface consists of a web application that guides the submitter through the data entry process to ensure that all of the required information is submitted. The submission is validated upon review, and a report is returned to the submitting organization, verifying either acceptance or rejection, based on the criteria requirements. For instance, Tier III and Tier IV checklists require validation using the SCAP Content Validation Tool (this tool is available for download via <http://scap.nist.gov/revision/1.2/#tools>).

The NCP is defined in SP 800-70 Revision 3, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, which can be found at <http://csrc.nist.gov/publications/PubsSPs.html>.

#### **For More Information, See:**

<https://checklists.nist.gov>

#### **CONTACT:**

Mr. Stephen Quinn  
(301) 975-6967  
[stephen.quinn@nist.gov](mailto:stephen.quinn@nist.gov)

## United States Government Configuration Baseline (USGCB) / FDCC Baselines

The United States Government Configuration Baseline (USGCB) initiative creates security configuration baselines for information technology (IT) products that are widely deployed across the federal agencies. The project originally evolved from the Federal Desktop Core Configuration (FDCC) mandate originally described in a March 2007 memorandum from OMB, Memorandum M-07-11. The purpose of the USGCB program is to help improve information security and reduce overall IT operating costs by providing commonly accepted and agreed upon security configurations for major operating systems and applications.

Through the NCP described in SP 800-70 Revision 3, a baseline submitter may express interest in submitting a candidate for use in the USGCB program.

CSD provides ongoing support for the USGCB automation content, including periodic updates to the existing content, encouraging vendors to submit candidates, assisting USGCB users in continuously monitoring and assessing security compliance of information systems within their environment. This ongoing monitoring element supports the Risk Management Framework described in SP 800-37 Revision 1. It also supports the Core functions of the Cybersecurity Framework, providing USGCB users with settings that protect digital assets and supports the detection of suspicious activity.

During FY 2016, the USGCB program will continue to provide ongoing maintenance of the baseline artifacts and to consider additional applicable platforms as authored and submitted by the platform vendors, as well as other organizations that wish to contribute candidate content.

### For More Information, See:

<http://usgcb.nist.gov>

### CONTACT:

Team email: [usgcb@nist.gov](mailto:usgcb@nist.gov)

Mr. Stephen Quinn

(301) 975-6967

[stephen.quinn@nist.gov](mailto:stephen.quinn@nist.gov)

## Apple OS X Security Configuration

CSD is working to develop secure system configuration baselines supporting different operational environments for Apple OS X Version 10.10, "Yosemite." These configuration guidelines will assist organizations with hardening OS X technologies and provide a basis for unified controls and settings for OS X workstations and for mobile system security configurations for federal agencies.

The configurations are based on a collection of resources, including the existing NIST OS X configuration guidance, the OS X security configuration guide, the Department of Defense (DOD) OS X Recommended Settings, and the Defense Information Systems Agency (DISA) OS X Security Technical Implementation Guide (STIG). The project team aggregated 400 initial settings, determined which settings to include in the configuration baseline, and determined appropriate values for each included setting. The desired configuration items have been established, and the team is continuing to develop shell scripts that apply the settings to an OS X 10.10 system. The settings are organized into three key baselines, which are appropriate for different environments:

- The Enterprise baseline is appropriate for centrally managed, networked systems;
- The Small Office Home Office baseline, sometimes called Standalone, describes small, informal computer installations that are used for home or business purposes; and
- The Specialized Security-Limited Functionality baseline is appropriate for systems where security requirements are more stringent and where the implementation of security safeguards is likely to reduce functionality.

SCAP, defined and discussed in an earlier section of this report, will be used to express configuration settings and check system configuration compliance.

During FY 2013, CSD provided a block of initial settings to Apple and these settings were posted for the Apple community on a periodic basis for public review, discussion, correction and agreement. Each setting has a designated Common Configuration Enumeration (CCE) number, which aids in the long-term tracking of the setting. Ultimately, the settings will be tested and included in the configuration baselines. In addition, CSD started the production of a draft guideline, *Guide to Securing Apple OS X 10.8 Systems for IT Professionals*. This guidance, which is similar in structure to the SP 800-68, *Windows XP Security Guide*, focuses on

providing detailed information about the security of Apple OS X, and providing security configuration guidelines for all users of the Apple OS X 10.8 operating system.

During FY 2014, a majority of all proposed settings were scripted. The corresponding spreadsheet batches have been sent to Apple for feedback; approximately 230 settings are now completed. Settings have also been implemented on OS X 10.9, when possible. Work on the draft guideline, *Guide to Securing Apple OS X 10.8 Systems for IT Professionals*, was temporarily suspended while configuration setting research was performed, but was resumed in FY 2015.

In FY 2015, CSD focused on the OS X 10.10 operating system for security testing. CSD finalized and tested the entire security configuration of 230 settings for OS X 10.10 and has continued updating the draft publication that was started for OS X 10.8 and has now been focused on OS X 10.10. For several months, one of the script's three profiles was deployed on select CSD systems for extensive testing. So far, results have been positive.

In FY 2016, CSD plans to release the draft publication, *Guide to Securing Apple OS X 10.10 Systems for IT Professionals*, for at least one public comment period, and plans to release a final version after incorporating changes from the comment period(s). CSD will continue to refine the script and add more settings to the configuration.

#### **For More Information, See:**

<http://csrc.nist.gov/projects/apple-os/>

## **CONTACTS:**

Mr. Mark Trapnell  
(301) 975-4091  
[mark.trapnell@nist.gov](mailto:mark.trapnell@nist.gov)

Mr. Lee Badger  
(301) 975-3176  
[lee.badger@nist.gov](mailto:lee.badger@nist.gov)

Mr. Murugiah Souppaya  
(301) 975-4102  
[murugiah.souppaya@nist.gov](mailto:murugiah.souppaya@nist.gov)

## **TECHNICAL SECURITY METRICS**

### **Security Risk Analysis of Enterprise Networks Using Attack Graphs**

The protection of computer networks from malicious intrusions is critical to the economy and security of the nation. Vulnerabilities are regularly discovered in software applications that are exploited to stage cyber attacks. System administrators need objective metrics to guide and justify decision making as they manage the security risk of enterprise networks. The objective of this research is to develop a standard model for the security risk analysis of computer networks. A standard model will enable NIST to answer questions such as "Are we more secure now than yesterday?" or "How does the security of one network configuration compare with another one?" Also, having a standard model to measure network security will allow users, vendors, and researchers to evaluate methodologies and products for network security in a coherent and consistent manner.

CSD has approached the challenge of network security analysis by capturing vulnerability interdependencies and measuring security, based on how real attackers have penetrated networks. CSD's methodology for security risk analysis is based on attack graphs. CSD analyzes attack paths through a network, providing a probabilistic metric of the overall system risk. Through this metric, CSD analyzes trade-offs between security costs and security benefits.

Computer systems are vulnerable to both known and zero-day attacks. Enterprises have begun to move parts of their networks from a traditional infrastructure into cloud computing environments. Cloud providers can offer virtual servers that can be rented on demand by users. This paradigm enables cloud customers to acquire computing resources with high efficiency, low cost and great flexibility. However, it also introduces many security problems that need to be solved.

In FY 2015, CSD attempted to model the problem of cloud security using a cloud-level attack graph. An attacker can create stealthy bridges (i.e., a covert connection between disparate networks that should be isolated) in a cloud environment. These stealthy bridges can be created using zero day vulnerabilities that cannot be detected by vulnerability scanners. The stealthy bridges can be used to construct a multi-step attack path and facilitate a subsequent intrusion process across enterprise islands in a cloud. CSD has developed a new technique to detect potential attacks in a Cloud using a probabilistic attack graph model. CSD



published a paper, *Inferring the Stealthy Bridges Between Enterprise Network Islands in Cloud Using Cross Layer Bayesian Networks*, for the Tenth International Conference on Security in Communication Networks, in Beijing, which was held October 24-26, 2015.

In FY 2016, CSD plans to develop new techniques and metrics to detect attacks on Cloud Computing and for network forensics analysis using Bayesian Networks. CSD also plans to publish the results as a NIST report and as white papers in conferences and journals.

**For More Information, See:**

<http://csrc.nist.gov/groups/SNS/security-risk-analysis-enterprise-networks/>

---

**CONTACT:**

Dr. Anoop Singhal  
(301) 975-4432  
anoop.singhal@nist.gov

**Algorithms for Intrusion Measurement**

The Algorithms for Intrusion Measurement (AIM) project furthers measurement science in designing and implementing algorithms to both detect attackers and limit their ability to intrude into a system. Most of the work leverages graph theory (the math of dots and lines) and algorithmic complexity analysis (the math around fast computation). In performing this work, the AIM project seeks to enhance the nation's ability to defend itself from network-borne attacks.

This scientific research is conducted in partnership with the Army Research Laboratory (ARL), the University of Maryland, and the Center for Applied Internet Data Analysis. ARL's participation helps focus the work on solving immediate critical problems facing U.S. Government networks. However, research solutions are made publicly available and are designed to be generally applicable to as many environments as possible.

In FY 2015, the AIM project completed research in several areas: measurements of Internet resilience of colluding country attacks, the optimal placement of defensive resources in Internet Protocol (IP) v6 networks, and circumvention-resistant network scan detection. More specifically, the project team accomplished the following:

- The team analyzed the resilience of the Internet with respect to countries colluding in using their influence over the Internet infrastructure to disconnect two

countries, isolate a set of countries from the Internet, or break the Internet up into non-communicating clusters (the research was published in the *International Journal of Computer Science: Theory and Applications*, as well as in the proceedings of the *Workshop for the Security of Emerging Network Technologies*).

- The research team showed how to leverage Internet Protocol Version 6 (IPv6) network migrations to enhance security capabilities. This was done through an evaluation of how to optimize the placement of defensive resources in specially secured IPv6 networks. The optimal placements best limit the movement of internal attackers to a small set of hosts or else force them to penetrate through the special security boundaries (the research was published in the journal *Data and Applications Security and Privacy*).
- In previous work, the team discovered a critical weakness in the most widely cited Threshold Random Walk (TRW) network scan detection algorithm that enabled a full circumvention by attackers. To mitigate the problem, we invented a scan detection methodology that will detect TRW circumvention activity and that also acts as an effective general-purpose scan detection algorithm. However, we find that the most effective approach is a composite solution that combines our approach with TRW (the research was published in the journal of *Security Informatics*).

In FY 2016, the AIM project will work on new methods for network anomaly detection, efficient representations for attack graphs, efficient computation of access control policy to restrict insider attacks, vertex partitioning on massive graphs to enable security resiliency analyses, and methods for using attack graphs to perform defense-in-depth measurements.

**For More Information, See:**

<http://csrc.nist.gov/projects/aim/>

---

**CONTACT:**

Mr. Peter Mell  
(301) 975-5572  
peter.mell@nist.gov

## Automated Combinatorial Testing

Software developers often encounter failures that result from an unexpected interaction between components. NIST research has shown that most failures are triggered by one or two parameters, and progressively fewer by three, four, or more parameters (see Figure 25 below), a relationship that is called the Interaction Rule. These results have important implications for testing. If all faults in a system can be triggered by a combination of  $n$  or fewer parameters, then testing all  $n$ -way combinations of parameters can provide very strong fault detection efficiency. These methods are being applied to software and hardware testing for reliability, safety, and security. CSD's focus is on empirical results and real-world problems.

Project highlights for FY 2015 include the publication of a paper on a new method of "oracle-free testing", a form of consistency checking using two-layer covering arrays with equivalence classes to automatically detect a large class of software faults; invited lectures at conferences and universities; leading the fourth International Workshop on Combinatorial Testing, held in conjunction with the eighth IEEE International Conference on Software Testing; initiating research on using combinatorial methods to reduce the cost of high assurance for life-critical software, tools and methods for locating faults from test results; and analyzing the factors involved in different types of software faults. Collaborators include researchers from the University of Texas at Arlington, the University of Texas at Dallas, East Carolina University, and Duke University.

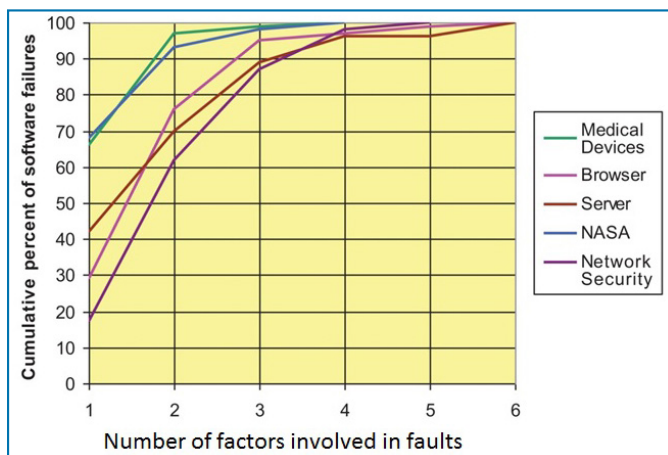


Figure 25: Interaction Rule Graph

Technology transfer activities included the publication of a number of technical papers and software distribution; publication of the results of a Cooperative R&D (CRADA) project with Lockheed Martin; release of enhanced

combinatorial measurement tools; input modeling and fault location tools; a provisional patent application on the oracle-free testing method; plus seminars at a number of conferences, universities, and federal agencies.

Plans for FY 2016 include combinatorial testing for big data software; initiation of a new CRADA project; measurement of input model combination coverage of security-critical software; a beta release of tools for testing to the modified condition decision coverage test criterion for life-critical software; developing tools to implement oracle-free testing methods; analysis of empirical data on failures; further development of methods and tools for fault localization; and seminars, workshops, and tutorials at professional meetings and research labs.

### For More Information, See:

<http://csrc.nist.gov/groups/SNS/acts/>

## CONTACTS:

Mr. Rick Kuhn  
(301) 975-3337  
kuhn@nist.gov


Dr. Raghu Kacker  
(301) 975-2109  
raghu.kacker@nist.gov

## Roots of Trust

Modern computing devices consist of various hardware, firmware, and software components at multiple layers of abstraction. Many security and protection mechanisms are currently rooted in software that, along with all underlying components, must be trusted and not tampered with. A vulnerability in any of those components could compromise the trustworthiness of the security mechanisms that rely upon those components. Stronger security assurances may be possible by grounding security mechanisms in roots of trust.

Roots of trust are highly reliable and secure hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by their design. As such, many roots of trust are implemented in hardware or protected firmware so that malware cannot tamper with the functions they provide. Roots of trust provide a firm foundation from which to build security and trust.

CSD's work aims to encourage the use of roots of trust in computers to provide stronger security assurances. A focus area for this work has been securing firmware. Previous guidelines by CSD described methods to protect boot firmware, commonly known as the Basic Input/Output System (BIOS) in PC clients and servers. In FY 2015, the first



of these guidelines, SP 800-147, *BIOS Protection Guidelines*, was submitted to ISO/IEC JTC 1/SC27 for standardization as ISO/IEC 19678:2015.

In FY 2016, CSD will continue to work with the computer industry on the use of roots of trust to improve the security of BIOS and other firmware. As part of this effort, CSD is researching techniques and requirements for securing firmware throughout the platform. This effort will consider methods to protect this firmware from unauthorized changes, detect accidental or malicious corruption, and recover from destructive attacks.

**For More Information, See:**

<http://csrc.nist.gov/projects/root-trust/>

---

**CONTACT:**

Mr. Andrew Regenscheid  
(301) 975-5155  
[andrew.regenscheid@nist.gov](mailto:andrew.regenscheid@nist.gov)



## HONORS AND AWARDS



# Department of Commerce

## Gold Medal Award

**Mr. Jon Boyens, Ms. Naomi Lefkovitz, Ms. Suzanne Lightman,  
Ms. Victoria Pillitteri, Mr. Matthew Scholl, and Mr. Kevin Stine  
Computer Security Division;  
Ms. Donna Dodson, and Mr. Adam Sedgewick, Information  
Technology Laboratory Office; and  
Ms. Lisa Carnahan, NIST Standards Coordination Office  
(former ITL team member)**



**Figure 26: Gold Medal Award Recipients**

**(left to right): Department of Commerce Deputy Secretary Bruce Andrews, Suzanne Lightman, Kevin Stine, Naomi Lefkovitz, Adam Sedgewick, Donna Dodson, Matthew Scholl, Victoria Pillitteri, Jon Boyens, and Dr. Willie May, Under Secretary of Commerce for Standards and Technology and NIST Director (Not Pictured: Lisa Carnahan)**

The group is recognized for its exceptional leadership and outstanding technical achievement in developing an innovative framework to improve the cybersecurity of our nation's critical infrastructure. In Executive Order 13636, the President directed NIST to create a Cybersecurity Framework to manage and reduce cybersecurity risk across the nation's critical infrastructure sectors. The team convened a highly diverse community to achieve consensus on a framework of standards, guidelines, and practices to identify, assess, and manage cybersecurity risk.

# Department of Commerce Silver Medal Award

**Mr. Richard Kuhn, Computer Security Division; and  
Dr. Raghu Kacker, Applied and Computational  
Mathematics Division**



**Figure 27: Silver Medal Award Recipients**

**(left to right): Department of Commerce Deputy Secretary Bruce Andrews, Richard Kuhn, Dr. Raghu Kacker, and Dr. Willie May, Under Secretary of Commerce for Standards and Technology and NIST Director**

The group is recognized for outstanding technical accomplishments in the development of the first efficient tool for generating high-strength software testing plans, resulting in cost savings and more reliable products. The team has developed software tools that use a novel combinatorial testing methodology. This methodology enables software developers to generate the smallest number of test cases needed to identify the most critical and elusive software bugs, those caused by interactions among input parameters. The team has made their tool, Automated Combinatorial Testing of Software (ACTS), widely available, and it is now used by major software companies and many government agencies.



## Dr. Ari Schwartz Receives Federal 100 Award

Ari Schwartz, ITL's Senior Internet Policy Advisor, who is on detail to the Executive Office of the President as the Senior Director for Cybersecurity, National Security Council, received a Federal 100 Award from Federal Computer Week. Dr. Schwartz was recognized for his deep knowledge and experience as a "voice of reason" and an advocate for a wide range of cybersecurity activities.



## Donna Dodson Named one of D.C.'s Top 50 Women in Technology

For the second year in a row, Donna Dodson has been named to D.C.'s Top 50 Women in Technology by FedScoop. Each year, FedScoop salutes a selection of D.C.'s Top Women in Technology, "whose vibrant energy, determination, imagination and leadership are making a monumental difference in the Federal Government IT community." Other notable recipients this year include Commerce Secretary Penny Pritzker and former NIST Director Arati Prabhakar.



**Figure 28: Department of Commerce Deputy Secretary Bruce Andrews (left) presents a Sammie Award to Dr. Ross on Oct. 7, 2015 in Washington, D.C.'s Andrew W. Mellon Auditorium.**

## NIST's Dr. Ron Ross Wins Three Top Awards for Advancing Cybersecurity

Dr. Ron Ross, leader of the Federal Information Security Management Act (FISMA) Implementation Project and an international cybersecurity ambassador, was recognized by three organizations for contributions to the field of cybersecurity:

- Dr. Ross was presented the **Samuel J. Heyman Service to America Medal** in the area of Homeland Security and Law Enforcement. The medal, often referred to as the "Sammie" award, is considered the "Oscar" award of government service. It highlights excellence in the federal workforce and inspires other talented and dedicated individuals to enter public service. He received the honor for "instituting a state-of-the-art risk assessment system that has protected federal computer networks from cyberattacks and helped secure information critical to our national and economic security."
- Government Computer News (GCN) magazine named Dr. Ross as **Government Executive of the Year** for his contributions to securing federal information systems.
- Dr. Ross was also inducted into the **National Cyber Security Hall of Fame**. The organization honors innovative individuals and organizations for their vision and leadership in creating foundational building blocks of the cybersecurity industry.

As a result of his widely used work, Dr. Ross has been called on by U.S. industry, academia and governments around the world to help their efforts to protect information. He has led U.S. cybersecurity teams to Australia, India, Japan, Canada, and the European Union, promoting effective information security concepts and best practices.

Credit: NIST Connections staff newsletter and Evelyn Brown, NIST Public Affairs Office



## Mr. Daniel Benigni Receives INCITS Lifetime Achievement Award

The InterNational Committee for Information Technology Standards (INCITS) organization presented Dan Benigni with a Lifetime Achievement Award in recognition of his continuous and outstandingly effective support for the development of standards in his role of managing the US Standards Committee on Cybersecurity (CS1).

This award is presented to only one INCITS participant annually, to a member who has demonstrated a long-time commitment to INCITS and its national and international standardization activities. The awardee must have demonstrated long-standing participation (ten or more years) in national and/or international standards development. Most importantly, it reflects the team spirit of the CS1 committee, whose members work together to reach the shared goal of promulgating security standards that will benefit U.S. industry and users over the long term.



## Mr. Randall (Randy) Easter Receives INCITS Technical Excellence Award

Mr. Easter was presented with the Technical Excellence Award, also from INCITS. INCITS is the primary U.S. forum dedicated to creating technology standards for innovation. This award is presented to no more than four participants to recognize visible and significant technical contributions to the work of a given national or international technical committee (TC), based upon a minimum of three years of TC participation by the awardee.





# COMPUTER SECURITY DIVISION PUBLICATIONS

## COMPUTER SECURITY DIVISION PUBLICATIONS

During FY 2015, CSD staff authored a significant number of computer, cyber, and/or information security-related standards, guidelines, recommendations and research findings through the NIST technical series, journal articles, conference papers, and other published documents.

In an effort to provide greater access to NIST's broad portfolio of security and privacy publications, CSD began posting additional Special Publications and NISTIRs on the CSRC that were developed by other components at NIST, such as the National Cybersecurity Center of Excellence (NCCoE) and National Strategy for Trusted Identities in Cyberspace (NSTIC). For example, CSRC now displays publications from the new NIST Cybersecurity Practice Guide series, SP 1800, authored by the NCCoE staff. The first three SP 1800 drafts were posted for public comment, describing work that closely relates to CSD standards, guidelines and research.

By posting cybersecurity and privacy draft publications from other NIST components on CSRC, CSD aims to provide greater visibility during public comment periods and to provide a primary resource for stakeholders to access a broad range of NIST cybersecurity and privacy publications.

In FY 2015, CSD posted a substantial number of final publications to CSRC, including two FIPS, fifteen Special Publications, and seven NISTIRs. The release of FIPS 202, *SHA-3 Standard*, in August 2015 was the culmination of many years of effort by the Cryptographic Technology Group to develop a next-generation standard for secure hashing. FIPS 202 specifies a family of fixed-length hash functions and extendable-output functions that complement the existing SHA-2 algorithms specified in FIPS 180-4, *Secure Hash Standard (SHS)*.

CSD continued to engage the public by posting fifteen SPs and thirteen NISTIRs as drafts for public comment. That included Draft NISTIR 8060, *Guidelines for the Creation of Interoperable Software Identification (SWID) Tags*, for which three iterations were released during short, two-week public comment periods. Comments were requested on three existing publications to determine what changes or approaches should be taken, prior to releasing an official draft for public comment. Those publications include i) SP 800-63-2, *Electronic Authentication Guideline*, ii) Security Content Automation Protocol (SCAP) version 1.3 and iii) the potential use of ISO/IEC 19790:2012 as the U.S. federal standard for cryptographic modules (as a potential successor to FIPS 140-2).

Publications are available for download from CSRC (<http://csrc.nist.gov/publications/>), including several NIST technical series:

- FIPS (<http://csrc.nist.gov/publications/PubsFIPS.html>);
- Special Publications (<http://csrc.nist.gov/publications/PubsSPs.html>);
- NISTIRs (<http://csrc.nist.gov/publications/PubsNISTIRs.html>); and
- ITL Bulletins (<http://csrc.nist.gov/publications/Pub-sITLSB.html>).

The following lists summarize some of the top CSD publications downloaded in FY 2015:

### Top 10 Most-Downloaded CSD Publications in NIST Technical Series (i.e., FIPS, SP 800s, NISTIRs, and ITL Bulletins):

1. SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;
2. SP 800-61 Revision 2, *Computer Security Incident Handling Guide*;
3. SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*;
4. SP 800-88 Revision 1, *Guidelines for Media Sanitization*;
5. SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*;
6. NISTIR 7298 Revision 2, *Glossary of Key Information Security Terms*;
7. SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*;
8. SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*;
9. SP 800-63-2, *Electronic Authentication Guideline*; and
10. SP 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*.

### Top 3 FIPS:

1. FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*;
2. FIPS 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*; and
3. FIPS 186-4, *Digital Signature Standard (DSS)*.

### Top 3 NISTIRs:

1. NISTIR 7298 Revision 2, *Glossary of Key Information Security Terms*;
2. NISTIR 7628 Revision 1, *Guidelines for Smart Grid Cyber Security*; and
3. NISTIR 8023, *Risk Management for Replication Devices*.

### Top 3 ITL Bulletins:

1. February 2015, *NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization*;
2. October 2014, *Release of NIST Special Publication 800-147B, BIOS Protection Guidelines for Servers*; and
3. January 2015, *Release of NIST Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations*.

Additionally, CSD shares its ongoing research efforts through other publications, such as journal articles, conference papers, books and other whitepapers. Although available through NIST's Publications Portal (<http://www.nist.gov/publication-portal.cfm>), they can also be accessed on CSRC's Articles page (<http://csrc.nist.gov/publications/articles/>). During FY 2015, more than 20 such documents were published, and are listed in the next section (FY 2015 Computer Security Division Publications) of this annual report.

In FY 2016, CSD plans to release a new version of CSRC that uses a content management system. The publications interface on the redesigned website will give users significantly greater capabilities for browsing, searching, downloading and sharing information on NIST's broad collection of computer security and privacy publications.

## FY 2015 Computer Security Division Publications

The Computer Security Division uses multiple NIST Technical Series to promulgate security standards, guidelines, recommendations, research, and additional background material. Those series include FIPS, SPs, NISTIRs and ITL Bulletins. Links to these publications are available at <http://csrc.nist.gov/publications>. As described earlier, in FY 2015, CSD began expanding its publication portfolio on CSRC by posting cybersecurity and privacy SPs and NISTIRs from other NIST components. In some cases, CSD staff contributed to the development of a publication (e.g., Draft SP 1800-3). Others were developed by other ITL cybersecurity components (e.g., NCCoE and NSTIC), documents that are closely related to CSD activities (e.g., Draft NISTIR 8062), or describe CSD programs and standardization activities within a greater context (e.g., Draft NISTIR 8074).

Additionally, each year CSD staff author numerous additional publications, including journal articles, conference papers, and other papers that are widely disseminated. They range from basic research to high-level summaries of CSD activities.

### NIST Technical Series Publications – FIPS, SPs, NISTIRs, and ITL Bulletins

Below are lists of NIST Technical Series publications that CSD released on CSRC as draft documents or as final publications during FY 2015 (from October 1, 2014 to September 30, 2015). Following the lists are abstracts for each publication.



## DRAFT PUBLICATIONS

**TABLE 3: NO DRAFT FIPS RELEASED DURING FY 2015**

**TABLE 4: SPECIAL PUBLICATIONS (SPs)**

Publication Number	Publication Title	Draft Released
SP 800-177	<i>Trustworthy Email</i>	September 2015
SP 800-171 (2nd Draft) (1st Draft)	<i>Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations</i>	April 2015 November 2014
SP 800-152	<i>A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)</i>	December 2014
SP 800-150	<i>Guide to Cyber Threat Information Sharing</i>	October 2014
SP 800-131A Rev. 1	<i>Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths</i>	July 2015
SP 800-125B	<i>Secure Virtual Network Configuration for Virtual Machine (VM) Protection</i>	September 2015
SP 800-125A	<i>Secure Recommendations for Hypervisor Deployment</i>	October 2014
SP 800-90A Rev. 1	<i>Recommendation for Random Number Generation Using Deterministic Random Bit Generators</i>	November 2014
SP 800-85A-4	<i>PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)</i>	June 2015
SP 800-82 Rev. 2 (2nd Draft)	<i>Guide to Industrial Control Systems (ICS) Security</i>	February 2015
SP 800-70 Rev. 3	<i>National Checklist Program for IT Products: Guidelines for Checklist Users and Developers</i>	March 2015
SP 800-57 Part 1 Rev. 4	<i>Recommendation for Key Management, Part 1: General</i>	September 2015
SP 1800-3	<i>Attribute Based Access Control</i>	September 2015
SP 1800-2	<i>Identity and Access Management for Electric Utilities</i>	August 2015
SP 1800-1	<i>Securing Electronic Health Records on Mobile Devices</i>	July 2015

**TABLE 5: NIST INTERAGENCY OR INTERNAL REPORTS (NISTIRs)**

Publication Number	Publication Title	Draft Released
NISTIR 8074	<i>Volume 1: Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity;</i> <i>Volume 2: Supplemental Information</i>	August 2015
NISTIR 8062	<i>Privacy Risk Management for Federal Information Systems</i>	May 2015
NISTIR 8060 (3rd Draft) (2nd Draft) (1st Draft)	<i>Guidelines for the Creation of Interoperable Software Identification (SWID) Tags</i>	August 2015 July 2015 May 2015



**TABLE 5 (CONT.): NIST INTERAGENCY OR INTERNAL REPORTS (NISTIRs)**

Publication Number	Publication Title	Draft Released
NISTIR 8058	<i>Security Content Automation Protocol (SCAP) Version 1.2 Content Style Guide: Best Practices for Creating and Maintaining SCAP 1.2 Content</i>	May 2015
NISTIR 8055	<i>Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research</i>	July 2015
NISTIR 8053	<i>De-Identification of Personally Identifiable Information</i>	April 2015
NISTIR 8050	<i>Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy: Summary and Next Steps</i>	April 2015
NISTIR 7966 (2nd Draft)	<i>Security of Interactive and Automated Access Management Using Secure Shell (SSH)</i>	March 2015
NISTIR 7904 (2nd Draft)	<i>Trusted Geolocation in the Cloud: Proof of Concept Implementation</i>	July 2015
NISTIR 7621 Rev. 1	<i>Small Business Information Security: the Fundamentals</i>	December 2014
NISTIR 7511 Rev. 4	<i>Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements</i>	September 2015

## FINAL APPROVED PUBLICATIONS

**TABLE 6: FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)**

Publication Number	Publication Title	Publication Date
FIPS 202	<i>SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions</i>	August 2015
FIPS 180-4	<i>Secure Hash Standard (SHS)</i> [updated Applicability section]	August 2015

**TABLE 7: SPECIAL PUBLICATIONS (SPs)**

Publication Number	Publication Title	Publication Date
SP 800-176	<i>Computer Security Division 2014 Annual Report</i>	August 2015
SP 800-171	<i>Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations</i>	June 2015
SP 800-163	<i>Vetting the Security of Mobile Applications</i>	January 2015
SP 800-161	<i>Supply Chain Risk Management Practices for Federal Information Systems and Organizations</i>	April 2015
SP 800-157	<i>Guidelines for Derived Personal Identity Verification (PIV) Credentials</i>	December 2014
SP 800-90A Rev. 1	<i>Recommendation for Random Number Generation Using Deterministic Random Bit Generators</i>	June 2015
SP 800-88 Rev. 1	<i>Guidelines for Media Sanitization</i>	December 2014

TABLE 7 (CONT.): SPECIAL PUBLICATIONS (SPs)		
Publication Number	Publication Title	Publication Date
SP 800-82 Rev. 2	<i>Guide to Industrial Control Systems (ICS) Security</i>	May 2015
SP 800-79-2	<i>Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)</i>	July 2015
SP 800-78-4	<i>Cryptographic Algorithms and Key Sizes for Personal Identity Verification</i>	May 2015
SP 800-73-4	<i>Interfaces for Personal Identity Verification</i>	May 2015
SP 800-57 Part 3 Rev. 1	<i>Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance</i>	January 2015
SP 800-53A Rev. 4	<i>Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans</i>	December 2014
SP 800-53 Rev. 4 (Update)	<i>Security and Privacy Controls for Federal Information Systems and Organizations</i>	January 2015
SP 500-304	<i>Conformance Testing Methodology Framework for ANSI/NIST-ITL 1-2011</i> Update: 2013, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information	June 2015

TABLE 8: NIST INTERAGENCY OR INTERNAL REPORTS (NISTIRs)		
Publication Number	Publication Title	Publication Date
NISTIR 8054	<i>NSTIC Pilots: Catalyzing the Identity Ecosystem</i>	April 2015
NISTIR 8041	<i>Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium</i>	April 2015
NISTIR 8023	<i>Risk Management for Replication Devices</i>	February 2015
NISTIR 8018	<i>Public Safety Mobile Application Security Requirements Workshop Summary</i>	January 2015
NISTIR 8014	<i>Considerations for Identity Management in Public Safety Mobile Networks</i>	March 2015
NISTIR 7863	<i>Cardholder Authentication for the PIV Digital Signature Key</i>	June 2015
NISTIR 7823	<i>Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework</i>	March 2015

TABLE 9: ITL BULLETINS	
Publication Date	Bulletin Title
September 2015	<i>Additional Secure Hash Algorithm Standards Offer New Opportunities for Data Protection</i>
August 2015	<i>Recommendation for Random Number Generation Using Deterministic Random Bit Generators</i>
July 2015	<i>Improved Security and Mobility Through Updated Interfaces for PIV Cards</i>
June 2015	<i>Increasing Visibility and Control of Your ICT Supply Chains</i>

**TABLE 9 (CONT.): ITL BULLETINS**

Publication Date	Bulletin Title
May 2015	<i>Authentication Considerations for Public Safety Mobile Networks</i>
April 2015	<i>Is Your Replication Device Making an Extra Copy for Someone Else?</i>
March 2015	<i>Guidance for Secure Authorization of Mobile Applications in the Corporate Environment</i>
February 2015	<i>NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization</i>
January 2015	<i>Release of NIST Special Publication 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations</i>
December 2014	<i>Release of NIST Special Publication 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials</i>
November 2014	<i>Cryptographic Module Validation Program (CMVP)</i>
October 2014	<i>Release of NIST Special Publication 800-147B, BIOS Protection Guidelines for Servers</i>

## ABSTRACTS OF NIST TECHNICAL SERIES PUBLICATIONS RELEASED IN FY 2015

The following sections provide abstracts for the draft and final FIPS, SPs, and security-related NISTIRs listed in the previous section. These publications are available at <http://csrc.nist.gov/publications>.

### FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)

#### **FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions**

This standard specifies the Secure Hash Algorithm-3 (SHA-3) family of functions on binary data. Each of the SHA-3 functions is based on an instance of the **Keccak** algorithm that NIST selected as the winner of the SHA-3 Cryptographic Hash Algorithm Competition. This standard also specifies the **Keccak-p** family of mathematical permutations, including the permutation that underlies **Keccak**, in order to facilitate the development of additional permutation-based cryptographic functions.

The SHA-3 family consists of four cryptographic hash functions, called SHA3-224, SHA3-256, SHA3-384, and SHA3-512, and two extendable-output functions (XOFs), called SHAKE128 and SHAKE256.

Hash functions are components for many important information security applications, including 1) the generation

and verification of digital signatures, 2) key derivation, and 3) pseudorandom bit generation. The hash functions specified in this standard supplement the SHA-1 hash function and the SHA-2 family of hash functions that are specified in FIPS 180-4, *Secure Hash Standard*.

Extendable-output functions are different from hash functions, but it is possible to use them in similar ways, with the flexibility to be adapted directly to the requirements of individual applications, subject to additional security considerations.

#### **FIPS 180-4 (Updated), Secure Hash Standard (SHS)**

This standard specifies SHA-1 and the SHA-2 family of hash algorithms that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated. The Applicability Clause of this standard was revised to correspond with the release of FIPS 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions* (see above). The revision to the Applicability Clause approves the use of hash functions specified in either FIPS 180-4 or FIPS 202 when a secure hash function is required for the protection of sensitive, unclassified information in federal applications, including as a component within other cryptographic algorithms and protocols.

### NIST SPECIAL PUBLICATIONS

#### **DRAFT SP 800-177, Trustworthy Email**

This document gives recommendations and guidelines for enhancing trust in email. The primary audience includes enterprise email administrators, information

security specialists and network managers. This guideline applies to federal IT systems and will also be useful for any small or medium sized organizations. Technologies recommended in support of the core Simple Mail Transfer Protocol (SMTP) and the Domain Name System (DNS) include mechanisms for authenticating a sending domain (Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC). Recommendations for email transmission security include Transport Layer Security (TLS) and associated certificate authentication protocols. Email content security is facilitated through the encryption and authentication of message content using Secure/Multipurpose Internet Mail Extensions (S/MIME) and OpenPGP, and associated certificate and key distribution protocols.

### **SP 800-176, Computer Security Division 2014 Annual Report**

Title III of the E-Government Act of 2002, titled the *Federal Information Security Management Act (FISMA)* of 2002, requires NIST to prepare an annual public report on activities undertaken in the previous year and planned for the coming year to carry out responsibilities under this law. The primary goal of the Computer Security Division, a component of NIST's Information Technology Laboratory, is to provide standards and technology that protects information systems against threats to the confidentiality, integrity, and availability of information and services. During Fiscal Year 2014, CSD successfully responded to numerous challenges and opportunities in fulfilling that mission. This annual report highlights the research agenda and activities in which CSD was engaged during FY 2014.

### **SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations**

The protection of Controlled Unclassified Information (CUI) while residing in nonfederal information systems and organizations is of paramount importance to federal agencies and can directly impact the ability of the Federal Government to successfully carry out its designated missions and business operations. This publication provides federal agencies with recommended requirements for protecting the confidentiality of CUI: (i) when the CUI is resident in nonfederal information systems and organizations; (ii) when the information systems where the CUI resides are not used or operated by contractors of federal agencies or other organizations on behalf of those agencies; and (iii) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for

the CUI category or subcategory listed in the CUI Registry. The requirements apply to all components of nonfederal information systems and organizations that process, store, or transmit CUI, or provide security protection for such components. The CUI requirements are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations.

### **SP 800-163, Vetting the Security of Mobile Applications**

Today's commercially available mobile devices (e.g., smartphones and tablets) are handheld computing platforms with wireless capabilities, geographic localization capabilities, cameras, and microphones. Similar to computing platforms such as desktops and laptops, the user experience with a mobile device is tied to the software apps and the tools and utilities available. The purpose of this document is to provide guidance for vetting third party software applications (apps) for mobile devices. Mobile app vetting is intended to assess a mobile app's operational characteristics of secure behavior and reliability (including performance) so that organizations can determine if the app is acceptable for use in their expected environment.

### **SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations**

Federal agencies are concerned about the risks associated with information and communications technology (ICT) products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the ICT supply chain. These risks are associated with the federal agencies decreased visibility into, understanding of, and control over how the technology that they acquire is developed, integrated and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services.

This publication provides guidance to federal agencies on identifying, assessing, and mitigating ICT supply chain risks at all levels of their organizations. This publication integrates ICT supply chain risk management (SCRM) into federal agency risk management activities by applying a multi-tiered, SCRM-specific approach, including guidance on supply chain risk assessment and mitigation activities.

### **SP 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials**

This recommendation provides technical guidelines for the implementation of standards-based, secure, reliable, interoperable public key infrastructure (PKI)-based identity credentials that are issued by federal departments and



agencies to individuals who possess and prove control over a valid PIV Card. The scope of this document includes requirements for initial issuance and maintenance of these credentials, certificate policies and cryptographic specifications, technical specifications for permitted cryptographic token types and the command interfaces for the removable implementations of such cryptographic tokens.

#### **DRAFT SP 800-152 (Third Draft), A Profile for U.S. Federal Cryptographic Key Management Systems (CKMS)**

This Profile for U.S. Federal Cryptographic Key Management Systems (FCKMSs) contains requirements for their design, implementation, procurement, installation, configuration, management, operation, and use by U.S. federal organizations. The Profile is based on SP 800-130, *A Framework for Designing Cryptographic Key Management Systems (CKMS)*.

#### **DRAFT SP 800-150, Guide to Cyber Threat Information Sharing**

In today's active threat environment, incident detection and response is an ongoing challenge for many organizations. This publication assists organizations in establishing computer security incident response capabilities that leverage the collective knowledge, experience, and abilities of their partners by actively sharing threat intelligence and ongoing coordination. This publication provides guidelines for coordinated incident handling, including producing and consuming data, participating in information sharing communities, and protecting incident-related data.

#### **DRAFT SP 800-131A Revision 1, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths**

At the start of the 21st Century, NIST began the task of providing cryptographic key management guidance, which includes defining and implementing appropriate key management procedures, using algorithms that adequately protect sensitive information, and planning ahead for possible changes in the use of cryptography because of algorithm breaks or the availability of more powerful computing techniques. NIST SP 800-57 Part 1 was the first document produced in this effort, and includes a general approach for transitioning from one algorithm or key length to another. This Recommendation (SP 800-131A) provides more specific guidance for transitions to the use of stronger cryptographic keys and more robust algorithms.

#### **DRAFT SP 800-125A, Secure Recommendations for Hypervisor Deployment**

The Hypervisor is a piece of software that provides the abstraction of all physical resources (such as CPU, Memory, Network and Storage) and thus, enables multiple computing stacks (consisting of an operating system, Middleware and Application programs) called Virtual Machines (VMs) to be run on a single physical host. In addition, a hypervisor may have the functionality to define a network within a single physical host (called a virtual network) to enable communication among the VMs resident on that host, as well as with physical and virtual machines outside the host. With all this functionality, the hypervisor is responsible for mediating access to physical resources, providing run-time isolation among resident VMs and enabling a virtual network that provides security-preserving communication flow among the VMs, and between the VMs and the external network. To design a hypervisor with the core functionality described above, there are architectural options, with each option presenting a different size of Trusted Computing Base (TCB) and hence, a different degree of ease in providing the required security assurance. Hence, in providing security recommendations for the hypervisor, two different approaches have been adopted in this document—one approach based on architectural options that provide more security assurance, and the second approach based on configuration choices that form part of its core administrative functions, such as the management of VMs, hypervisor host, hypervisor software and virtual networks.

#### **DRAFT SP 800-125B, Secure Virtual Network Configuration for Virtual Machine (VM) Protection**

Virtual Machines (VMs) are key resources to be protected, since they are the compute engines hosting mission-critical applications. Since VMs are end-nodes of a virtual network, the configuration of the virtual network forms an important element in the security of VMs and their hosted applications. The virtual network configuration areas discussed in this document are: Network Segmentation, Network path redundancy, firewall deployment architectures and VM Traffic Monitoring. The various configuration options under these areas are analyzed for their advantages and disadvantages, and a set of security recommendations are provided.

#### **SP 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators**

This Recommendation specifies mechanisms for the generation of random bits using deterministic methods. The methods provided are based on either hash functions or block cipher algorithms.

### **SP 800-88 Revision 1, *Guidelines for Media Sanitization***

Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. This guide will assist organizations and system owners in making practical sanitization decisions, based on a categorization of the confidentiality of their information.

### **DRAFT SP 800-85A-4, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance)***

SP 800-73 contains the technical specifications to interface with the smart card to retrieve and use the PIV identity credentials. This document, SP 800-85A, contains the test assertions and test procedures for testing smart card middleware as well as the card application. The tests reflect the design goals of interoperability and PIV Card functions.

### **SP 800-82 Revision 2, *Guide to Industrial Control Systems (ICS) Security***

This document provides guidance on how to secure Industrial Control Systems (ICS), including Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations, such as Programmable Logic Controllers (PLC), while addressing their unique performance, reliability, and safety requirements. The document provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

### **SP 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)***

The purpose of this SP is to provide appropriate and useful guidelines for assessing the reliability of issuers of PIV Cards and Derived PIV Credentials. These issuers store personal information and issue credentials based on OMB policies and on the standards published in response to HSPD-12 and, therefore, are the primary target of the assessment and authorization under this guideline. The reliability of an issuer is of utmost importance when one organization (e.g., a federal agency) is required to trust the identity credentials of individuals that were created and issued by another federal agency. This trust will only exist if organizations relying on the credentials issued by a given organization have the necessary level of assurance that the reliability of the issuing organization has been established through a formal authorization process.

### **SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification***

FIPS 201-2 defines requirements for the PIV lifecycle activities, including identity proofing, registration, PIV Card issuance, and PIV Card usage. FIPS 201-2 also defines the structure of an identity credential that includes cryptographic keys. This document contains the technical specifications needed for the mandatory and optional cryptographic keys specified in FIPS 201-2, as well as the supporting infrastructure specified in FIPS 201-2 and the related SP 800-73-4, *Interfaces for Personal Identity Verification*, and SP 800-76-2, *Biometric Specifications for Personal Identity Verification*, that rely on cryptographic functions.

### **SP 800-73-4, *Interfaces for Personal Identity Verification***

FIPS 201 defines the requirements and characteristics of a government-wide interoperable identity credential. FIPS 201 also specifies that this identity credential must be stored on a smart card. This document, SP 800-73, contains the technical specifications to interface with the smart card to retrieve and use the PIV identity credentials. The specifications reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying a PIV data model, card edge interface, and application programming interface. The specifications go further by constraining implementers' interpretations of the normative standards. Such restrictions are designed to ease implementation, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications.

### **DRAFT SP 800-70 Revision 3, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers***

A security configuration checklist is a document that contains instructions or procedures for configuring an IT product for an operational environment, for verifying that the product has been configured properly, and/or for identifying unauthorized changes to the product. Using these checklists can minimize the attack surface, reduce vulnerabilities, lessen the impact of successful attacks, and identify changes that might otherwise go undetected. To facilitate the development of checklists and to make checklists more organized and usable, NIST established the National Checklist Program (NCP). This publication explains how to use the NCP to find and retrieve checklists, and it also describes the policies, procedures, and general requirements for participation in the NCP.

## **DRAFT SP 800-57 Part 1 Revision 4, *Recommendation for Key Management, Part 1: General***

SP 800-57 Part 1 contains basic key management guidance. The document:

1. Defines the security services that may be provided and key types that may be employed in using cryptographic mechanisms;
2. Provides background information regarding the cryptographic algorithms that use cryptographic keying material;
3. Classifies the different types of keys and other cryptographic information according to their functions, specifies the protection that each type of information requires and identifies methods for providing this protection;
4. Identifies the states in which a cryptographic key may exist during its lifetime;
5. Identifies the multitude of functions involved in key management; and
6. Discusses a variety of key management issues related to the keying material. Topics discussed include key usage, cryptoperiod length, domain-parameter validation, public-key validation, accountability, audit, key management system survivability, and guidance for cryptographic algorithm and key size selection.

## **SP 800-57 Part 3 Revision 1, *Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance***

SP 800-57 Part 3 is intended primarily to help system administrators and system installers adequately secure applications, based on product availability and organizational needs and to support organizational decisions about future procurements. This document also provides information for end users regarding application options left under their control in normal use of the application. Recommendations are given for a select set of applications: Public Key Infrastructures (PKI), Internet Protocol Security (IPsec), Transport Layer Security (TLS), Secure/Multipurpose Internet Mail Extensions (S/MIME), Kerberos, Over-the-Air Rekeying of Digital Radios (OTAR), Domain Name System Security Extensions (DNSSEC), Encrypted File Systems (EFS), and Secure Shell (SSH).

## **SP 800-53A Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans***

This publication provides a set of procedures for conducting assessments of the security controls and privacy controls employed within federal information systems and

organizations. The assessment procedures, executed at various phases of the system development life cycle, are consistent with the security and privacy controls in SP 800-53 Revision 4. The procedures are customizable and can be easily tailored to provide organizations with the needed flexibility to conduct security control assessments and privacy control assessments that support organizational risk management processes and that are aligned with the stated risk tolerance of the organization. Information on building effective security assessment plans and privacy assessment plans is also provided, along with guidance on analyzing assessment results.

## **SP 800-53 Rev. 4 (Update), *Security and Privacy Controls for Federal Information Systems and Organizations***

This publication provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats, including hostile cyber attacks, natural disasters, structural failures, and human errors (both intentional and unintentional). The security and privacy controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the Federal Government and critical infrastructure that are derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. The publication also describes how to develop specialized sets of controls, or overlays, that are tailored for specific types of missions/business functions, technologies, or environments of operation. Finally, the catalog of security controls addresses security from both a functionality perspective (the strength of security functions and mechanisms provided) and an assurance perspective (the measures of confidence in the implemented security capability). Addressing both security functionality and assurance helps to ensure that information technology component products and the information systems built from those products using sound system and security engineering principles are sufficiently trustworthy.

## **SP 500-304, *Conformance Testing Methodology Framework for ANSI/NIST-ITL 1-2011 Update: 2013, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information***

Conformance testing measures whether an implementation faithfully implements the technical requirements defined in a standard. Conformance testing provides developers, users, and purchasers with increased levels of confidence in



product quality and increases the probability of successful interoperability. The CSD developed a conformance testing methodology framework for ANSI/NIST-ITL 1-2011 Update: 2013, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information (AN-2013)*. This testing methodology framework defines the test assertions implemented within CSD's conformance test tool, which is designed to test implementations of AN-2013 transactions and promotes biometrics conformity assessment efforts. This initial document includes comprehensive tables of AN-2013 requirements and test assertions for transaction-wide requirements and Record Type 1 (which is required for all transactions). The tables of requirements and assertions indicate which assertions apply to the traditional encoding format, the National Information Exchange Model (NIEM)-compliant encoding format, or both encoding formats. The testing methodology framework defines and makes use of a specific test assertion syntax, which clearly defines the assertions associated with each requirement.

#### **DRAFT SP 1800-3, Attribute Based Access Control**

Enterprises rely upon strong access control mechanisms to ensure that corporate resources (e.g., applications, networks, systems and data) are not exposed to anyone other than an authorized user. As business requirements change, enterprises need highly flexible access control mechanisms that can adapt. The application of attribute-based policy definitions enables enterprises to accommodate a diverse set of business cases. This NCCoE practice guide details a collaborative effort between the NCCoE and technology providers to demonstrate a standards-based approach to attribute-based access control (ABAC).

This guide discusses potential security risks facing organizations, benefits that may result from the implementation of an ABAC system and the approach that the NCCoE took in developing a reference architecture and build. Included is a discussion of major architecture design considerations, an explanation of security characteristics achieved by the reference design and a mapping of security characteristics to applicable standards and security control families.

For parties interested in adopting all or part of the NCCoE reference architecture, this guide includes a detailed description of the installation, configuration and integration of all components.

#### **DRAFT SP 1800-2, Identity and Access Management for Electric Utilities**

To protect power generation, transmission, and distribution, energy companies need to control physical and logical access to their resources, including buildings, equipment,

information technology, and industrial control systems. They must authenticate authorized individuals to the devices and facilities to which they are giving access rights with a high degree of certainty. In addition, they need to enforce access control policies (e.g., allow, deny or inquire further) consistently, uniformly, and quickly across all of their resources. This project resulted from a direct dialogue among NCCoE staff and members of the electricity subsector, mainly from electric power companies and those who provide equipment and/or services to them.

The goal of this project is to demonstrate a centralized, standards-based technical approach that unifies identity and access management (IdAM) functions across operational technology (OT) networks, physical access control systems (PACS), and information technology systems. These networks often operate independently, which can result in identity and access information disparity, increased costs, inefficiencies, and loss of capacity and service delivery capability. This guide describes the collaborative efforts with technology providers and electric company stakeholders to address the security challenges that energy providers face in the core function of IdAM. It offers a technical approach to meeting the challenge, and also incorporates a business value mind-set by identifying the strategic considerations involved in implementing new technologies.

This Cybersecurity Practice Guide provides a modular, open, end-to-end example solution that can be tailored and implemented by energy providers of varying sizes and sophistication. It shows energy providers how NIST met the challenge using open source and commercially available tools and technologies that are consistent with cybersecurity standards. The use case scenario is based on a normal day-to-day business operational scenario that provides the underlying impetus for the functionality presented in the guide. While the reference solution was demonstrated with a certain suite of products, the guide does not endorse these products in particular. Instead, it presents the characteristics and capabilities that an organization's security experts can use to identify similar standards-based products that can be integrated quickly and cost-effectively with an energy provider's existing tools and infrastructure.

#### **DRAFT SP 1800-1, Securing Electronic Health Records on Mobile Devices**

Health care providers increasingly use mobile devices to receive, store, process, and transmit patient clinical information. According to NIST's risk analysis, discussed here, and in the experience of many health care providers, mobile devices can present vulnerabilities in a health care organization's networks. At the 2012 Health and Human Services Mobile Devices Roundtable, participants stressed



that mobile devices are being used by many providers for health care delivery before they have implemented safeguards for privacy and security.

This Cybersecurity Practice Guide provides a modular, open, end-to-end reference design that can be tailored and implemented by health care organizations of varying sizes and information technology sophistication. Specifically, the guide shows how health care providers, using open source and commercially available tools and technologies that are consistent with cybersecurity standards, can more securely share patient information among caregivers using mobile devices. The scenario considered is that of a hypothetical primary care physician using her mobile device to perform reoccurring activities, such as sending a referral (e.g., clinical information) to another physician, or sending an electronic prescription to a pharmacy. While the design was demonstrated with a certain suite of products, the guide does not endorse these products in particular. Instead, it presents the characteristics and capabilities that an organization's security experts can use to identify similar standards-based products that can be integrated quickly and cost-effectively with a health care provider's existing tools and infrastructure.

## NISTIRS

### **DRAFT NISTIR 8074 (2 VOLUMES):**

**Volume 1: Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity**

#### **Volume 2: Supplemental Information**

This report sets out proposed United States Government (USG) strategic objectives for pursuing the development and use of international standards for cybersecurity and makes recommendations to achieve those objectives. The recommendations cover interagency coordination, collaboration with the U.S. private sector and international partners, agency participation in international standards development, standards training and education, the use of international standards to achieve mission and policy objectives, and other issues. NISTIR 8074 Volume 2, *Supplemental Information for the Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity*, provides additional background on international cybersecurity standardization.

### **DRAFT NISTIR 8062, *Privacy Risk Management for Federal Information Systems***

This document describes a privacy risk management framework for federal information systems. The framework provides the basis for the establishment of a common vocabulary to facilitate a better understanding of and communication about privacy risks and the effective implementation of privacy principles in federal information systems. This publication focuses on the development of two key pillars to support the application of the framework: privacy engineering objectives and a privacy risk model.

### **DRAFT NISTIR 8060 (Three drafts), *Guidelines for the Creation of Interoperable Software Identification (SWID) Tags***

This guidance provides an overview of the capabilities and usage of Software Identification (SWID) tags as part of a comprehensive software life cycle. As instantiated in the International Organization for Standardization (ISO)/International Electrotechnical Commission (ISO/IEC) 19770-2 standard, SWID tags support numerous applications for software asset management and information security management. This report introduces SWID tags in an operational context, provides guidelines for the creation of interoperable SWID tags, and highlights key usage scenarios for which SWID tags are applicable.

### **DRAFT NISTIR 8058, *Security Content Automation Protocol (SCAP) Version 1.2 Content Style Guide: Best Practices for Creating and Maintaining SCAP 1.2 Content***

The Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the format and nomenclature by which software flaw and security configuration information is communicated, both to machines and humans. SCAP version 1.2 requirements are defined in SP 800-126 Revision 2. Over time, certain stylistic conventions regarding the authoring of SCAP 1.2 content have become best practices. While these best practices are not required, they improve the quality of the SCAP content in several ways, such as improving the accuracy and consistency of results, avoiding performance problems, reducing user effort, lowering content maintenance burdens, and enabling content reuse. This document has been created to capture the best practices and encourage their use by SCAP content authors and maintainers.

### **DRAFT NISTIR 8055, *Derived Personal Identity Verification (PIV) Credentials (DPC) Proof of Concept Research***

This report documents a proof-of-concept implementation for Derived PIV Credentials (DPCs). Smart card-based PIV Cards cannot be readily used with most mobile devices,

such as smartphones and tablets, but DPCs can be used instead to PIV-enable these devices and provide multi-factor authentication for mobile device users. This report captures existing requirements related to DPCs, proposes an architecture that supports these requirements, and then demonstrates how such an architecture could be implemented and operated.

#### **NISTIR 8054, *NSTIC Pilots: Catalyzing the Identity Ecosystem***

Pilots are an integral part of the National Strategy for Trusted Identities in Cyberspace (NSTIC), passed by the White House in 2011 to encourage enhanced security, privacy, interoperability, and ease-of-use for online transactions. This document details summaries and outcomes of NSTIC pilots; in addition, it explores common themes in the pilots' work, developing and operating innovative identity solutions.

#### **DRAFT NISTIR 8053, *De-Identification of Personally Identifiable Information***

De-identification removes identifying information from a dataset so that individual data cannot be linked with specific individuals. De-identification can reduce the privacy risk associated with collecting, processing, archiving, distributing or publishing information. De-identification thus attempts to balance the contradictory goals of using and sharing personal information, while protecting privacy. Several U.S. laws, regulations and policies specify that data should be de-identified prior to sharing. In recent years, researchers have shown that some de-identified data can sometimes be re-identified. Many different kinds of information can be de-identified, including structured information, free format text, multimedia, and medical imagery. This document summarizes roughly two decades of de-identification research, discusses current practices, and presents opportunities for future research.

#### **DRAFT NISTIR 8050, *Executive Technical Workshop on Improving Cybersecurity and Consumer Privacy: Summary and Next Steps***

Cybersecurity incidents have grown swiftly from conceivable to realized risks that regularly threaten the national and economic security of the United States. These risks threaten the financial security of companies and the public, weaken consumer confidence, erode individual privacy protections, and damage the brand value and reputation of businesses. On February 12, 2015, NIST and Stanford University hosted an executive technical workshop, which was held in coordination with the White House Summit on Cybersecurity and Consumer Protection, to discuss how to increase the use of advanced cybersecurity and privacy technologies in consumer-facing organizations. This document details the

discussion and ideas presented at the workshop and serves as a platform to receive broader feedback on the relevance of projects and suggestions discussed at that event.

#### **NISTIR 8041, *Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium***

Direct Digital Manufacturing (DDM) involves fabricating physical objects from a data file using computer-controlled processes with little to no human intervention. It includes Additive Manufacturing (AM), 3D printing, rapid prototyping, etc. The technology is advancing rapidly and has the potential to significantly change traditional manufacturing and supply chain industries, including information and communication technologies (ICT). On February 3, 2015, CSD hosted a one-day symposium to explore the cybersecurity needed for DDM, to include ensuring the protection of intellectual property and the integrity of printers, elements being printed, and design data. Speakers and attendees from industry, academia, and government discussed the state of the industry, cybersecurity risks and solutions, and implications for ICT supply chain risk management (SCRM).

#### **NISTIR 8023, *Risk Management for Replication Devices***

This publication provides guidance on protecting the confidentiality, integrity, and availability of information processed, stored, or transmitted on replication devices (RDs). It suggests appropriate countermeasures in the context of the System Development Life Cycle (SDLC). A security risk assessment template in table and flowchart format is also provided to help organizations determine the risk associated with replication devices.

#### **NISTIR 8018, *Public Safety Mobile Application Security Requirements Workshop Summary***

This document captures the input received from the half-day workshop, "Public Safety Mobile Application Security Requirements," organized by the Association of Public-Safety Communications Officials (APCO) International, in cooperation with FirstNet and the Department of Commerce and held on February 25, 2014. This first-of-its-kind workshop was attended by public safety practitioners, mobile application developers, industry experts, and government officials who contributed their experience and knowledge to provide input in identifying security requirements for public safety mobile applications.

#### **NISTIR 8014, *Considerations for Identity Management in Public Safety Mobile Networks***

This document analyzes approaches to identity management for public safety networks in an effort to assist individuals developing technical and policy requirements for public safety use. These considerations are scoped into the context of their applicability to public safety communications

networks, with a particular focus on the nationwide public safety broadband network (NPSBN) based on the Long Term Evolution (LTE) family of standards. A short background on identity management is provided alongside a review of applicable federal and industry guidance. Considerations are provided for identity proofing, selecting tokens, and the authentication process. While specific identity management technologies are analyzed, the document does not preclude other identity management technologies from being used in public safety communications networks.

#### **DRAFT NISTIR 7966 (Second Draft), *Security of Interactive and Automated Access Management Using Secure Shell (SSH)***

Users and hosts must be able to access other hosts in an interactive or automated fashion, often with very high privileges, for a variety of reasons, including file transfers, disaster recovery, privileged access management, software and patch management, and dynamic cloud provisioning. This is often accomplished using the Secure Shell (SSH) protocol. The SSH protocol supports several mechanisms for interactive and automated authentication. Management of this access requires proper provisioning, termination, and monitoring processes. However, the security of SSH key-based access has been largely ignored to date. This publication assists organizations in understanding the basics of SSH interactive and automated access management in an enterprise, focusing on the management of SSH user keys.

#### **DRAFT NISTIR 7904 (Second Draft), *Trusted Geolocation in the Cloud: Proof of Concept Implementation***

This publication explains selected security challenges involving Infrastructure as a Service (IaaS) cloud computing technologies and geolocation. It then describes a proof-of-concept implementation that was designed to address those challenges. The publication provides sufficient details about the proof-of-concept implementation so that organizations can reproduce it if desired. The publication is intended to be a blueprint or template that can be used by the general security community to validate and implement the described proof-of-concept implementation.

#### **NISTIR 7863, *Cardholder Authentication for the PIV Digital Signature Key***

FIPS 201-2 requires explicit user action by the PIV cardholder as a condition for the use of the digital signature key stored on the card. This document clarifies the requirement for explicit user action to encourage the development of compliant applications and middleware that use the digital signature key.

#### **NISTIR 7823, *Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework***

As electric utilities turn to Advanced Metering Infrastructures (AMIs) to promote the development and deployment of the Smart Grid, one aspect that can benefit from standardization is the upgradeability of Smart Meters. The National Electrical Manufacturers Association (NEMA) standard SG-AMI1-2009, “Requirements for Smart Meter Upgradeability,” describes functional and security requirements for the secure upgrade – both local and remote – of Smart Meters. This report describes conformance test requirements that may be used voluntarily by testers and/or test laboratories to determine whether Smart Meters and Upgrade Management Systems conform to the requirements of NEMA SG-AMI 1-2009. For each relevant requirement in NEMA SG-AMI 1-2009, the document identifies the information to be provided by the vendor to facilitate testing, and the high-level test procedures to be conducted by the tester/laboratory to determine conformance.

#### **DRAFT NISTIR 7621 Revision 1, *Small Business Information Security: the Fundamentals***

NIST, as a partner with the Small Business Administration and the Federal Bureau of Investigation in an information security awareness outreach to the small business community, developed this NISTIR as a reference guideline for small businesses. This document is intended to present the fundamentals of a small business information security program in non-technical language.

#### **DRAFT NISTIR 7511 Revision 4, *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements***

This report defines the requirements and associated test procedures necessary for products or modules to achieve one or more Security Content Automation Protocol (SCAP) validations. Validation is awarded, based on a defined set of SCAP capabilities by independent laboratories that have been accredited for SCAP testing by the NIST National Voluntary Laboratory Accreditation Program (NVLAP).

## **ADDITIONAL PUBLICATIONS BY CSD AUTHORS**

CSD authors actively contribute to the security community by authoring articles in scholarly literature, participating in technical conferences, contributing to encyclopedias and other books, and publishing other “white papers” that fall outside the scope of NIST Technical Series publications described above.



The following documents were published during FY 2015. For conference papers, the contributions listed below were either i) accepted for a conference held during FY 2015, or ii) accepted for a conference held prior to FY 2015, with a final proceeding published in FY 2015 (and not listed in an earlier CSD Annual Report). All NIST authors (as listed for an individual publication) are identified using *italics*.

Links to the preprints and/or final publications of the documents below are available at <http://csrc.nist.gov/publications/articles>.

## Journal Articles

E. Andreeva, C. Bouillaguet, O. Dunkelman, P.-A. Fouque, J. Hoch, J. Kelsey, A. Shamir, and S. Zimmer, "New Second-Preimage Attacks on Hash Functions," *Journal of Cryptology*, 40 pp. (June 23, 2015). doi: 10.1007/s00145-015-9206-4.

In this work, we present several new generic second-preimage attacks on hash functions. Our first attack is based on the herding attack and applies to various Merkle-Damgård-based iterative hash functions. Compared to the previously known long-message second-preimage attacks, our attack offers more flexibility in choosing the second-preimage message at the cost of a small computational overhead. More concretely, our attack allows the adversary to replace only a few blocks in the original target message to obtain the second preimage. As a result, our new attack is applicable to constructions previously believed to be immune to such second-preimage attacks. Among others, these include the dithered hash proposal of Rivest, Shoup's UOWHF, and the ROX constructions. In addition, we also suggest several time-memory-data tradeoff attack variants, allowing for a faster online phase, and even finding second preimages for shorter messages. We further extend our attack to sequences stronger than the ones suggested in Rivest's proposal. To this end, we introduce the kite generator as a new tool to attack any dithering sequence over a small alphabet. Additionally, we analyze the second-preimage security of the basic tree hash construction. We also propose several second-preimage attacks and their time-memory-data tradeoff variants. Finally, we show how both our new and the previous second-preimage attacks can be applied even more efficiently when multiple short messages, rather than a single long target message, are available.

M. Chang, D. R. Kuhn and T. Weil, "IT Security," *IT Professional* 17(1), 14-15 (January/February 2015). doi: 10.1109/MITP.2015.10.

How can IT professionals adapt to ever-changing security challenges quickly and without draining

their organizations' resources? Articles in this issue highlight emerging trends and suggest ways to approach and address cybersecurity challenges.

J. Hagar, T. Wissink, D. R. Kuhn and R. Kacker, "Introducing Combinatorial Testing in a Large Organization," *Computer (IEEE Computer)* 48(4), 64-72 (April 2015). doi: 10.1109/MC.2015.114.

A two-year study of eight pilot projects to introduce combinatorial testing in a large aerospace corporation found that the new methods were practical, significantly lowered development costs, and improved test coverage by 20 to 50 percent.

R. Harang and P. M. Mell, "Evasion-Resistant Network Scan Detection," *Security Informatics* 4(4), 1-10 (May 2015). doi: 10.1186/s13388-015-0019-7.

Popular network scan detection algorithms operate through evaluating external sources for unusual connection patterns and traffic rates. Research has revealed evasive tactics that enable full circumvention of existing approaches (specifically the widely cited Threshold Random Walk algorithm). To prevent the use of these circumvention techniques, we propose a novel approach to network scan detection that evaluates the behavior of internal network nodes, and combine it with other established techniques of scan detection. By itself, our algorithm is an efficient, protocol-agnostic, completely unsupervised method that requires no a priori knowledge of the network being defended beyond which hosts are internal and which hosts are external to the network, and is capable of detecting network scanning attempts, regardless of the rate of the scan (working even with connectionless protocols). We demonstrate the effectiveness of our method on both live data from an enterprise-scale network and on simulated scan data, finding a false positive rate of just 0.000034 % with respect to the number of inbound flows. When combined with both Threshold Random Walk and simple rate-limiting detection, we achieve an overall detection rate of 94.44 %.

D. R. Kuhn, R. Kacker and Y. Lei, "Combinatorial Coverage as an Aspect of Test Quality," *Crosstalk (Hill AFB): the Journal of Defense Software Engineering* 28(2), 19-23 (March/April 2015).

There are relatively few good methods for evaluating test set quality after ensuring basic requirements traceability. Structural coverage, mutation testing, and related methods can be used if source code is available, but these approaches may entail significant



cost in time and resources. This paper introduces an alternative measure of test quality that is directly related to fault detection, simple to compute, and can be applied prior to the execution of the system under test. As such, it provides an inexpensive complement to current approaches for evaluating test quality.

J. Luna, N. Suri, M. Iorga and A. Karmel, "Leveraging the Potential of Cloud Security Service-Level Agreements through Standards," *IEEE Cloud Computing* 2(3), 32-40 (May-June 2015). doi: 10.1109/MCC.2015.52.

Despite the undisputed advantages of cloud computing, customers – in particular, small and medium enterprises – still need a meaningful understanding of the security and risk-management changes that the cloud entails so that they can assess whether this new computing paradigm meets their security requirements. This article presents a fresh view on this problem by surveying and analyzing, from the standardization and risk assessment perspective, the specification of security in cloud service-level agreements as a promising approach to empower customers in assessing and understanding cloud security. Apart from analyzing the proposed risk-based approach and surveying the relevant landscape, this article presents a real-world scenario to support the creation and adoption of service-level agreements as enablers for negotiating, assessing, and monitoring the achieved security levels in cloud services.

P. M. Mell, R. Harang and A. Gueye, "Measuring Limits on the Ability of Colluding Countries to Partition the Internet," *International Journal of Computer Science: Theory and Application* 3(3), 60-73 (2015).

We show that the strength of the Internet-based network interconnectivity of countries is increasing over time. We then evaluate bounds on the extent to which a group of colluding countries can disrupt this connectivity. We evaluate the degree to which a group of countries can disconnect two other countries, isolate a set of countries from the Internet, or even break the Internet up into non-communicative clusters. To do this, we create an interconnectivity map of the worldwide Internet routing infrastructure at a country-level of abstraction. We then examine how groups of countries may use their pieces of routing infrastructure to filter out the traffic of other countries (or to block entire routes). Overall, bounds analysis indicates that the ability of countries to perform such disruptions to connectivity has diminished significantly between 2008 and 2013. However, we show that the majority of the gains in robustness go

to countries that had already displayed significant robustness to the types of attacks that we consider. The countries that displayed higher initial vulnerability to such attacks did not become significantly more robust over the time period of analysis.

D. Moody, R. Peralta, R. Perlner, A. Regenscheid, A. Roginsky and L. Chen, "Report on Pairing-based Cryptography," *Journal of Research of the National Institute of Standards and Technology* 120, 11-27 (2015). doi: 10.6028/jres.120.002.

This report summarizes study results on pairing-based cryptography. The main purpose of the study is to form NIST's position on standardizing and recommending the pairing-based cryptographic schemes currently published in research literature and standardized in other standards development organizations. The report reviews the mathematical background of pairings. This includes topics such as pairing-friendly elliptic curves and how to compute various pairings. The report includes a brief introduction on existing identity-based encryption (IBE) schemes and other cryptographic schemes using pairing technology. The report provides a complete study of the current status of standards activities on pairing-based cryptographic schemes and explores different application scenarios for pairing-based cryptographic schemes. As an important aspect of adopting pairing-based schemes, the report also considers the challenges inherent in CAVP and CMVP testing for FIPS 140 validation. Based on the study, the report suggests an approach for including pairing-based cryptographic schemes in the NIST cryptographic toolkit. The report also outlines several questions that will require further study if this approach is followed.

D. Moody and D. Shumow, "Analogues of Vélu's Formulas for Isogenies on Alternate Models of Elliptic Curves," *Mathematics of Computation*, 23 pp. (September 9, 2015). doi: 10.1090/mcom/3036.

Isogenies are the morphisms between elliptic curves and are, accordingly, a topic of interest in the subject. As such, they have been well studied, and have been used in several cryptographic applications. Vélu's formulas show how to explicitly evaluate an isogeny, given a specification of the kernel as a list of points. However, Vélu's formulas only work for elliptic curves specified by a Weierstrass equation. This paper presents formulas similar to Vélu's that can be used to evaluate isogenies on Edwards curves and Huff curves, which are normal forms of elliptic curves that provide an alternative to the traditional Weierstrass form. Our formulas are not simply compositions

of Vélú's formulas with mappings to and from Weierstrass form. Our alternate derivation yields efficient formulas for isogenies with lower algebraic complexity than such compositions. In fact, these formulas have lower algebraic complexity than Vélú's formulas on Weierstrass curves.

D. Moody, D. Smith-Tone and S. Paul, "Improved Indifferentiability Security Bound for the JH Mode," *Designs, Codes and Cryptography* 74(3), 23 pp. (February 2015). doi: 10.1007/s10623-015-0047-9.

Indifferentiability security of a hash mode of operation guarantees the mode's resistance against all generic attacks. It is also useful to establish the security of protocols that use hash functions as random functions. The JH hash function was one of the five finalists in NIST's SHA-3 hash function competition. Despite several years of analysis, the indifferentiability security of the JH mode has remained remarkably low, only at  $n/3$  bits, while the two finalist modes **Keccak** and **Grøstl** offer a security guarantee of  $n/2$  bits. Note that all these three modes operate with an  $n$ -bit digest and  $2n$ -bit permutations. In this paper, we improve the indifferentiability security bound for the JH mode to  $n/2$  bits (e.g., from approximately 171 to 256 bits when  $n = 512$ ). To put this into perspective, our result guarantees the absence of (non-trivial) attacks on both the JH-256 and JH-512 hash functions with time less than approximately  $2^{256}$  computations of the underlying 1024-bit permutation, under the assumption that the underlying permutations can be modeled as an ideal permutation. Our bounds are optimal for JH-256, and the best-known bound for JH-512. We obtain this improved bound by establishing an isomorphism of certain query-response graphs through a careful design of the simulators and bad events. Our experimental data strongly supports the theoretically obtained results.

A.T. Vassilev and C. Celli, "Avoiding Cyberspace Catastrophes through Smarter Testing," *Computer (IEEE Computer)* 47(10), 102-106 (October 2014). doi: 10.1109/MC.2014.47.

The Heartbleed bug highlighted a critical problem in the software industry: inadequately tested software results in serious security vulnerabilities. Available testing technologies, combined with emerging standards, can help tech companies meet increasing consumer demand for greater Internet security.

## Conference Papers

J. Boyar and M. Find, "Constructive Relationships Between Algebraic Thickness and Normality," *20th International*

*Symposium on Fundamentals of Computation Theory (FCT 2015)*, Gdańsk, Poland, August 17-19, 2015. In Lecture Notes in Computer Science 9210, *Fundamentals of Computation Theory*, A. Kosowski and I. Walukiewicz, eds., Berlin: Springer International, 2015, pp. 106-117. doi: 10.1007/978-3-319-22177-9\_9.

We study the relationship between two measures of Boolean functions; "algebraic thickness" and "normality". For a function  $f$ , the algebraic thickness is a variant of the "sparsity", the number of nonzero coefficients in the unique  $F_2$  polynomial representing  $f$  and the normality is the largest dimension of an affine subspace on which  $f$  is constant. We show that for  $0 < \epsilon < 2$ , any function with algebraic thickness  $n^{3-\epsilon}$  is constant on some affine subspace of dimension  $\Omega(n^\epsilon)$ . Furthermore, we give an algorithm for finding such a subspace. This is at most a factor of  $\Theta(\sqrt{n})$  from the best guaranteed, and when restricted to the technique used, is at most a factor of  $\Theta(\sqrt{\log n})$  from the best guaranteed. We also show that a concrete function, majority, has algebraic thickness  $\Omega(2^{n^{1/6}})$ .

R. Chandramouli, "Analysis of Network Segmentation Techniques in Cloud Data Centers," *2015 International Conference on Grid & Cloud Computing and Applications (GCA '15)*, Las Vegas, Nevada, United States, July 27-30, 2015, pp. 64-70.

Cloud Data centers are predominantly made up of Virtualized hosts. The networking infrastructure in a cloud (virtualized) data center, therefore, consists of the combination of a physical IP network (data center fabric) and the virtual network residing in virtualized hosts. Network Segmentation (Isolation), Traffic flow control using firewalls and Intrusion Detection Systems / Intrusion Protection Systems (IDS/IPS) form the primary network-based security techniques, with the first one as the foundation for the other two. In this paper, we describe and analyze three generations of network segmentation techniques—Virtual Switches and Physical NIC-based, VLAN-based and Overlay-based. We take a detailed look at the overlay-based virtual network segmentation and its characteristics, such as scalability and ease of configuration.

R. Chandramouli, "Deployment-driven Security Configuration for Virtual Networks," *6th International Conference on Networks & Communications (NETCOM 2014)*, Chennai, India, December 27-28, 2014, pp. 1-13. doi: 10.5121/csit.2014.41301.

Virtualized Infrastructures are increasingly deployed in many data centers. One of the key components of this virtualized infrastructure is the virtual network

– a software-defined communication fabric that links together the various Virtual Machines (VMs) to each other and to the physical host on which the VMs reside. Because of its key role in providing connectivity among VMs and the applications hosted on them, Virtual Networks have to be securely configured to provide the foundation for the overall security of the virtualized infrastructure in any deployment scenario. The objective of this paper is to illustrate a deployment-driven methodology for deriving a security configuration for Virtual Networks. The methodology outlines two typical deployment scenarios, identifies use cases and their associated security requirements, discusses the security solutions to meet those requirements and the virtual network security configuration to implement each security solution, and then analyzes the pros and cons of each security solution.

D. R. Kuhn, R. N. Kacker, Y. Lei and J. Torres-Jimenez, "Equivalence Class Verification and Oracle-Free Testing Using Two-layer Covering Arrays," *Fourth International Workshop on Combinatorial Testing (IWCT 2015) in Proceedings of the 2015 IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, Graz, Austria, April 13-17, 2015, 4 pp. doi: 10.1109/ICSTW.2015.7107445.

This short paper introduces a method for verifying equivalence classes for module/unit testing. This is achieved using a two-layer covering array in which some or all values of a primary covering array represent equivalence classes. A second-layer covering array of the equivalence class values is computed, and its values substituted for the equivalence class names in the primary array. It is shown that this method can detect certain classes of errors without a conventional test oracle, and an illustrative example is given.

P. M. Mell and R. Harang, "Lightweight Packing of Log Files for Improved Compression in Mobile Tactical Networks," *Military Communications Conference (MILCOM 2014)*, Baltimore, Maryland, United States, October 6-8, 2014, pp. 192-197. doi: 10.1109/MILCOM.2014.37.

Devices in mobile tactical edge networks are often resource constrained, due to their lightweight and mobile nature, and often have limited access to bandwidth. In order to maintain situational awareness in the cyber domain, security logs from these devices must be transmitted to command and control sites. We present a lightweight packing step that takes advantage of the restricted semantics and regular

format of certain kinds of log files to render them substantially more amenable to compression with standard algorithms (especially Lempel-Ziv variants). We demonstrate that we can reduce compressed file sizes to as little as 21 % of that of the maximally compressed file without packing. We can also reduce overall compression times up to 64 % in our data sets. Our packing step permits a lossless transmission of larger log files across the same network transmission medium, as well as permitting existing sets of logs to be transmitted within smaller network availability windows.

P. M. Mell, R. Harang and A. Gueye, "The Resilience of the Internet to Colluding Country Induced Connectivity Disruptions," *Security of Emerging Networking Technologies (SENT) Workshop at the 2015 Network and Distributed System Security Symposium (NDSS '15)*, San Diego, California, United States, February 8-11, 2015, 10 pp. doi: 10.14722/sent.2015.23007.

We show that the strength of Internet-based network interconnectivity of countries is increasing over time. We then evaluate bounds on the extent to which a group of colluding countries can disrupt this connectivity. We evaluate the degree to which a group of countries can disconnect two other countries, isolate a set of countries from the Internet, or even break the Internet up into non-communicative clusters. To do this, we create an interconnectivity map of the worldwide Internet routing infrastructure at a country-level of abstraction. We then examine how groups of countries may use their pieces of routing infrastructure to filter out the traffic of other countries (or to block entire routes). Overall, bounds analysis indicates that the ability of countries to perform such disruptions to connectivity has diminished significantly between 2008 and 2013. However, we show that the majority of the gains in robustness go to countries that had already displayed significant robustness to the types of attacks that we consider. The countries that displayed higher initial vulnerability to such attacks did not become significantly more robust over the time period of analysis.

D. Moody, R. Perlner and D. Smith-Tone, "An Asymptotically Optimal Structural Attack on the ABC Multivariate Encryption Scheme," *6th International Workshop on Post-Quantum Cryptography (PQCrypto 2014)*, Waterloo, Ontario, Canada, October 1-3, 2014. In *Lecture Notes in Computer Science 8772, Post-Quantum Cryptography*, M. Mosca, ed., Berlin: Springer International, 2014, pp. 180-196. doi: 10.1007/978-3-319-11659-4\_11.

Historically, multivariate public key cryptography has been less than successful at offering encryption schemes that are both secure and efficient. At PQCRYPTO '13 in Limoges, Tao, Diene, Tang, and Ding introduced a promising new multivariate encryption algorithm based on a fundamentally new idea: hiding the structure of a large matrix algebra over a finite field. We present an attack based on the subspace differential invariants inherent to this methodology. The attack is a structural key recovery attack that is asymptotically optimal among all known attacks (including algebraic attacks) on the original scheme and its generalizations.

A. Nelson and S. Garfinkel, "Measuring Systematic and Random Error in Digital Forensics" [abstract], *International Symposium on Forensic Science Error Management: Detection, Measurement and Mitigation*, Arlington, Virginia, United States, July 21-24, 2015, 1 p.

Recognized sources of error in digital forensics include systematic errors arising from implementation errors, and random errors resulting from faulty equipment. But as digital forensic techniques expand to include statistical machine learning, another source of error will be statistical errors that arise because of chance disagreements between a statistical model and subject systems examined with that model. We consider two digital forensics systems with these different types of measurable error.

First, we show a mechanism for comparing the numerous and nuanced results of parsing a file system. Multiple storage system parsers were designed for or adapted to analyze a game console with a custom file system. However, it was initially unknown whether any of the parsers would produce a perspective of the storage system that was correct in reporting the files present and their characteristics. We adapted the parsers to produce an in-common, machine-differentiable format, and used a storage differencing algorithm to measure the relative incorrectness of each of the parsers. Discrepancies summarize errors in implementation or specification, an important report when any reverse-engineering is necessary. We discuss advantages and challenges in adopting this practice.

Second, we show how to construct a classifier using the hard drive from a multi-user computer that can determine the user responsible for creating a file. The classifier is constructed using allocated files and its accuracy determined with take-one-out cross-validation. Once created, the classifier can be used to

predict the creator of files that can only be recovered with carving.

R. Perlner, "Optimizing Information Set Decoding Algorithms to Attack Cyclosymmetric MDPC Codes," *6th International Workshop on Post-Quantum Cryptography* (PQCrypto 2014), Waterloo, Ontario, Canada, October 1-3, 2014. In *Lecture Notes in Computer Science 8772, Post-Quantum Cryptography*, M. Mosca, ed., Berlin: Springer International, 2014, pp. 220-228. doi: 10.1007/978-3-319-11659-4\_13.

Recently, several promising approaches have been proposed to reduce key sizes for code-based cryptography using structured, but non-algebraic codes, such as quasi-cyclic (QC) Moderate Density Parity Check (MDPC) codes. Biasi et al. propose further reducing the key sizes of code-based schemes using cyclosymmetric (CS) codes. While Biasi et al. analyze the complexity of attacking their scheme using standard information-set-decoding algorithms, the research presented here shows that information set decoding algorithms can be improved, by choosing the columns of the information set in a way that takes advantage of the added symmetry. The result is an attack that significantly reduces the security of the proposed CS-MDPC schemes to the point that they no longer offer an advantage in key size over QC-MDPC schemes of the same security level. QC-MDPC schemes are not affected by this paper's result.

M. Sönmez Turan and J. Kelsey, "How Random is Your RNG?" *Shmooscon 2015*, Washington, DC, United States, January 16-18, 2015, 4 pp.

Cryptographic primitives need random numbers to protect your data. Random numbers are used for generating secret keys, nonces, random paddings, initialization vectors, salts, etc. Deterministic pseudorandom number generators are useful, but they still need truly random seeds generated by entropy sources in order to produce random numbers. Researchers have shown examples of deployed systems that did not have enough randomness in their entropy sources, and as a result, cryptographic keys were compromised. So how do you know how much entropy is in your entropy source? Estimating entropy is a difficult (if not impossible) problem, and we've been working to create usable guidance that will give conservative estimates on the amount of entropy in an entropy source. From our research, we shared some of the challenges and proposed methods. In addition, we discussed some of the new directions that we are investigating, and present results of our estimation methods on simulated entropy sources.



## Books and Book Sections

F. Herr, and F. L. Podio, "Common Biometric Exchange Formats Framework Standardization," in *Encyclopedia of Biometrics*, 2nd ed. Edited by S. Z. Li and A. Jain. New York: Springer Reference, 2015.

The Common Biometric Exchange Formats Framework (CBEFF) provides a standardized set of definitions and procedures that support the interchange of biometric data in standard data structures called CBEFF biometric information records (BIRs). CBEFF permits considerable flexibility regarding BIR structures and biometric data content, but does so in a way that makes it easy for biometric applications to evaluate their interest in processing a particular BIR. At their conceptually simplest, standard CBEFF data structures promote the interoperability of biometric-based application programs and systems by specifying a standardized wrapper for describing, at a high level, the format and certain attributes of the content of a BIR. The initial versions of CBEFF were developed by NIST and the Biometric Consortium. The CBEFF specification published by NIST in April 2004 (NISTIR 6529-A) was proposed as the basis for the development of formal national and international CBEFF standards. Since then, American National Standards and International Standards (ISO/IEC) have been published. Development continues at the international level on a new generation of CBEFF standards. The paper describes the main characteristics of CBEFF, emphasizing the value of CBEFF data structures in open and complex biometric systems, especially in cases where the system must cope with a wide variety of biometric data records, some of which may even be encrypted. It provides adoption examples of CBEFF data structures by national and international organizations and programs, and discusses early work on CBEFF standardization. Recent and current standardization efforts are addressed.

D. J. Yaga, J. Campbell and G. Zekster, "Conformance Testing Methodologies for Biometric Data Interchange Formats, Standardization of," in *Encyclopedia of Biometrics*, 2nd ed. Edited by S. Z. Li and A. Jain. New York: SpringerReference, 2015.

Conformance testing is the method that is used to determine if a product, process or system (known as an implementation under test) satisfies the requirements specified in the base standard. The goal of conformance testing is to capture enough of the requirements of the base standard and test them

under enough conditions that any implementation under test that passes the conformance test is likely to be conformant. Conformance testing provides developers, users, and purchasers with increased levels of confidence in product quality and increases the probability of successful interoperability. Conformance testing methodology standards for data interchange formats identify a language to define the context of conformance testing and conformance claims. These standards include the set of requirements specified in the base standards and one or more conformance test assertions per requirement. There are several efforts in biometric conformance test standardization, including U.S. national organizations, such as International Committee for Information Technology Standards Technical Committee M1-Biometrics and NIST, who is responsible for the development of the ANSI/NIST-ITL standards; and international organizations, such as the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) Joint Technical Commission 1, Subcommittee 37 - Biometrics. The paper includes a description of the different national and international efforts that have taken place in the last few years in the development of conformance testing methodologies for biometric data interchange formats developed by the organizations mentioned above. The content of these standards (for both published standards and ongoing projects) are addressed.

## White Papers

M. Dworkin and R. Perlner, "Analysis of VAES3 (FF2)," *Cryptology ePrint Archive* [Website], Report 2015/306, April 2, 2015. Available at: <http://eprint.iacr.org/2015/306>.

This note describes a theoretical chosen-plaintext attack on the VAES3 mode for format-preserving encryption. VAES3 was specified under the name FF2 in Draft National Institute of Standards and Technology (NIST) Special Publication 800-38G, *Recommendation for Block Cipher Modes of Operation: Methods for Format-Preserving Encryption*.

## ACRONYMS

3D	Three-Dimensional
3GPP	3rd Generation Partnership Project
ABAC	Attribute Based Access Control
AC	Access Control
ACD	Applied Cybersecurity Division
ACM	Association for Computing Machinery
ACPT	Access Control Policy Tool
ACRLCS	AC Rule Logic Circuit Simulation
ACTS	Advanced Combinatorial Testing System
AES	Advanced Encryption Standard
AIM	Algorithms for Intrusion Measurement
AM	Additive Manufacturing
AMI	Advanced Metering Infrastructure
ANSs	American National Standards
ANSI	American National Standards Institute
APCO	Association of Public-Safety Communications Officials
API	Application Programming Interface
ARF	Asset Reporting Format
ARL	Army Research Laboratory
ASC	Accredited Standards Committee
ASC X9, Inc.	Accredited Standards Committee X9, Inc.
ASKDF	Application-Specific Key Derivation functions
BioAPI	Biometric Application Programming Interface
BioCTS	Biometric Conformance Test Software
BIOS	Basic Input/Output System
BIRs	biometric information records
BT-SEG	Bluetooth Security Expert Group
CAC	Common Access Card
CAE	Centers of Academic Excellence
CAVP	Cryptographic Algorithm Validation Program

CBEFF	Common Biometric Exchange Formats Framework
CCE	Common Configuration Enumeration
CCEVS	Common Criteria Evaluation and Validation Scheme
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CCSS	Common Configuration Scoring System
CDH	Confactor Diffie-Hellman
CDM	Continuous Diagnostics and Mitigation
CERT	Computer Emergency Readiness Team
CHES	Cryptographic Hardware and Embedded Systems
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CKMS	Cryptographic Key Management System
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CNCI	Comprehensive National Cybersecurity Initiative
CNSS	Committee on National Security Systems
CompTIA	Computing Technology Industry Association
COV	Committee of Visitors
CPE	Common Platform Enumeration
CPS	Cyber-Physical Systems
CPU	Central Processing Unit
CRADA	Cooperative Research and Development Agreement
CS1	Cyber Security 1
CSCRM	Cyber Supply Chain Risk Management
CSD	Computer Security Division
CSE	Communications Security Establishment
CSF	Cybersecurity Framework
CSIA	Cyber Security and Information Assurance
CSRC	Computer Security Resource Center
CSRIC	Communications Security, Reliability and Interoperability Council

CSSPAB	Computer System Security and Privacy Advisory Board	EO	Executive Order
CST	Cryptographic and Security Testing	ESDC	Employment and Social Development Canada
CSWG	Cybersecurity Working Group	ETSI	European Telecommunications Standards Institute
CTG	Cryptographic Technology Group		
CUI	Controlled Unclassified Information	FAA	Federal Aviation Administration
CVE	Common Vulnerabilities and Exposures	FAQ	Frequently Asked Questions
CVSS	Common Vulnerability Scoring System	FAR	Federal Acquisition Regulation
		FBI	Federal Bureau of Investigation
DAPS	Distributed application platforms and services	FCCX	Federal Cloud Credential Exchange
DARPA	Defense Advanced Research Projects Agency	FCKMSs	Federal Cryptographic Key Management Systems
DCS	Distributed Control Systems	FCSM	Federal Computer Security Managers
DDM	Direct Digital Manufacturing	FDA	Federal Drug Administration
DFO	Designated Federal Officer	FDCC	Federal Desktop Core Configuration
DH	Diffie-Hellman	FedRAMP	Federal Risk and Authorization Management Program
DHS	Department of Homeland Security	FEMA	Federal Emergency Management Agency
DHHS	Department of Health and Human Services	FFRDCs	Federally Funded Research and Development Centers
DKIM	Domain Keys Identified Mail	FIPS	Federal Information Processing Standard
DMARC	Domain based Message Authentication, Reporting and Conformance	FIRST	Forum of Incident Response and Security Teams
DNS	Domain Name System	FirstNet	First Responder Network Authority
DNSSEC	Domain Name System Security Extensions	FISMA	Federal Information Security Management Act
DOD	Department of Defense	FISSEA	Federal Information Systems Security Educators' Association
DoS	Department of State		
DOT	Department of Transportation	FPE	Format-Preserving Encryption
DPC	Derived PIV Credentials	FR	Federal Register
DPCI	Derived PIV Credential Issuers	FY	Fiscal Year
DRBG	Deterministic Random Bit Generator		
DSS	Digital Signature Standard	GAO	Government Accountability Office
DTR	Derived Test Requirements	GCM	Galois/Counter Mode
		GCN	Government Computer News
EAC	Election Assistance Commission	GCSE	Group Communication System Enablers
EaaS	Entropy as a Service	GICS	Generic Identity Command Set
ECC	Elliptic Curve Cryptography	GPS	Global Positioning System
ECDSA	Elliptic Curve Digital Signature Algorithm	GSA	General Services Administration
ECP	Enterprise Compliance Profile		
EL	Engineering Laboratory		
EM	Encoded Message		

HAVA	Help America Vote Act	IT	Information Technology
HIT	Health information technology	ITI	Information Technology Industry
HIPAA	Health Insurance Portability and Accountability Act	ITL	Information Technology Laboratory
HMAC	Hash-based Message Authentication Code	ITU-T	International Telecommunications Union – Telecommunication Standardization Sector
HSPD-12	Homeland Security Presidential Directive-12	IUT	Implementation under test
		IWCE	International Wireless Communications Expo
IaaS	Infrastructure as a Service	IWG	Interagency Working Group
IAD	Information Access Division		
IAPWG	Information Assurance Policy Working Group	JTF	Joint Task Force
IBE	Identity-based Encryption	JTC 1	Joint Technical Committee 1
IC	Intelligence Community		
ICC	Integrated Circuit Card	KBKDF	Key-Based Key Derivation functions
ICS	Industrial Control Systems	KDF	Key Derivation Functions
ICSTW	International Conference on Software Testing, Verification and Validation Workshops	LDS	Logical Data Structure
ICT	Information and Communications Technology	LTE	Long-Term Evolution
IdAM	Identity and Access Management	MCPTT	Mission Critical Push-To-Talk
IEC	International Electrotechnical Commission	MILCOM	Military Communications Conference
IEEE	Institute of Electrical and Electronics Engineers	MIH	Media-Independent Handover
IETF	Internet Engineering Task Force	MLS	Multi-Level Security
IG	Implementation Guidance	MMT	Multi-Block Message Test
IGs	Inspector Generals	MQV	Menezes-Qu-Vanstone
IKE	Internet Key Exchange		
IMS	Innovation in Measurement Science	NARA	National Archives and Records Administration
INCITS	InterNational Committee for Information Technology Standards	NASA	National Aeronautics and Space Administration
IP	Internet Protocol	NASPO	North American Security Products Organization
IPD	Initial Public Draft	NCCoE	National Cybersecurity Center of Excellence
IPv6	Internet Protocol Version 6	NCP	National Checklist Program
ISA	International Society of Automation	NCWF	National Cybersecurity Workforce Framework
ISO	International Organization for Standardization	NEMA	National Electrical Manufacturers Association
ISP	Internet Service Provider		
ISPAB	Information Security and Privacy Advisory Board	NFC	Near Field Communications



NGAC	Next Generation Access Control	PIV	Personal Identity Verification
NGAC-FA	Next Generation Access Control – Functional Architecture	PIV-I	PIV-Interoperable
NGAC-GOADS	Next Generation Access Control – Generic Operations & Abstract Data Structures	PKCS	Public Key Cryptography Standards
NGAC-IRPADS	Next Generation Access Control Implementation Requirements, Protocols and API Definitions	PKI	Public Key Infrastructure
NICE	National Initiative for Cybersecurity Education	P.L.	Public Law
NIEM	National Information Exchange Model	PLC	Programmable Logic Controllers
NISTIR	NIST Interagency Report	PM	Policy Machine
NITRD	Networking and Information Technology Research and Development	PML	Physical Measurement Laboratory
NPIVP	NIST Personal Identity Verification Program	PoS	Point of Service
NPSBN	National Public Safety Broadband Network	PPD	Presidential Policy Directive
NSA	National Security Agency	PQC	Post-Quantum Cryptography
NSTIC	National Strategy for Trusted Identities in Cyberspace	PRNGs	Pseudorandom Number Generators
NTIA	National Telecommunications and Information Administration	ProSe	Proximity Services
NVD	National Vulnerability Database	PSCR	Public Safety Communications Research
NVLAP	National Voluntary Laboratory Accreditation Program	PSS	Probabilistic Signature Scheme
NYU	New York University	PUB	Publication
OCIL	Open Checklist Interactive Language	PWG	Public Working Group
OCR	Office for Civil Rights	RBAC	Role-Based Access Control
ODNI	Office of the Director of National Intelligence	RBG	Random Bit Generator
ODP	Open Distributed Processing	RD	Replication Device
OMB	Office of Management and Budget	R&D	Research and Development
OPM	Office of Personnel Management	RFC	Request for Comments
OT	Operational Technology	RFI	Request for Information
OVAL	Open Vulnerability and Assessment Language	RFID	Radio Frequency Identification
PACS	Physical Access Control Systems	RMF	Risk Management Framework
PCI	Payment Card Industry	RNG	Random Number Generation
PCLOB	Privacy and Civil Liberties Oversight Board	RSA	Rivest, Shamir, Adleman
PIN	Personal Identification Number	SACM	Security Automation and Continuous Monitoring
		SBA	Small Business Administration
		SBIR	Small Business Innovation Research
		SC	Subcommittee
		SCADA	Supervisory Control and Data Acquisition
		SCAP	Security Content Automation Protocol
		SCAPVal	SCAP Content Validation Tool
		SCMG	Security Components and Mechanisms Group

SCORE	Special Cyber Operations Research and Engineering	TIC	Trusted Internet Connection
SCRM	Supply Chain Risk Management	TLS	Transport Layer Security
SDLC	System Development Life Cycle	TMSAD	Trust Model for Security Automation Data
SDO	Standards Developing Organizations	TNC	Trusted Network Communications
SENT	Security of Emerging Networking Technologies	TPM	Trusted Platform Module
SGCC	Smart Grid Cybersecurity Committee	TRW	Threshold Random Walk
SGIP	Smart Grid Interoperability Panel	TS	Technical Standard
SHA	Secure Hash Algorithm	TTPs	Tactics, Techniques, and Procedures
SHS	Secure Hash Standard	U.S.C.	U.S. Code
SIG	Special Interest Group	US-CERT	U.S. Computer Emergency Readiness Team
SLAs	Service Level Agreements	USG	U.S. Government
SMB	Small and Medium-size Business	USGCB	United States Government Configuration Baseline
SMEs	Small and Medium Enterprises	USGv6	U.S. Government IPv6
S/MIME	Secure/Multipurpose Internet Mail Extensions	USNC	United States National Committee
SMTP	Simple Mail Transfer Protocol	UX	User experience
SNMP	Simple Network Management Protocol	VA	Veteran Affairs
SOIG	Security Outreach and Integration Group	VCAT	Visiting Committee on Advanced Technology
SP	Special Publications	VCI	Virtual Contact Interface
SPF	Sender Policy Framework	VM	Virtual Machine
SRTP	Secure Real-time Transport Protocol	VPN	Virtual Private Network
SSA	Social Security Administration	VRDX-SIG	Vulnerability Reporting and Data eXchange SIG
SSAG	Secure Systems and Applications Group	VVSG	Voluntary Voting System Guidelines
SSCA	Software and Supply Chain Assurance	WG	Working Group
SSD	Software and Systems Division	Wi-Fi	Wireless Fidelity
SSH	Secure Shell	XACML	eXtensible Access Control Markup Language
STVM	Security Testing, Validation, and Measurement	XCCDF	Extensible Configuration Checklist Description Format
STVMG	Security Testing, Validation, and Measurement Group	XML	Extensible Markup Language
SWID	Software Identification	XOFs	Extendable-Output Functions
TAG	Technical Advisory Group	xTract	Threat Reduction and Correlation Tool
TCG	Trusted Computing Group	XTS	XEX Tweakable Block Cipher with Ciphertext Stealing
TDEA	Triple Data Encryption Algorithm		
TDES	Triple Data Encryption Standard		
TGDC	Technical Guidelines Development Committee		

## OPPORTUNITIES TO ENGAGE WITH CSD, ACD, AND NIST

### Guest Research Internships at NIST

Opportunities are available at NIST for 6- to 24-month internships within the Computer Security Division (CSD) and the Applied Cybersecurity Division (ACD). Qualified individuals should contact CSD and/or ACD, provide a statement of qualifications, and indicate the area of work that is of interest. The salary costs are generally borne by the sponsoring institution; however, in some cases, these guest research internships carry a small monthly stipend paid by NIST. For further information, contact:

CSD Contact:

Mr. Matthew Scholl  
(301) 975-2941  
matthew.scholl@nist.gov

ACD Contact:

Mr. Kevin Stine  
(301) 975-4483  
kevin.stine@nist.gov

### Details at NIST for Government or Military Personnel

Opportunities are available at NIST for 6- to 24-month details at NIST in CSD and/or ACD. Qualified individuals should contact CSD and/or ACD, provide a statement of qualifications, and indicate the area of work that is of interest. Generally speaking, the salary costs are borne by the sponsoring agency; however, in some cases, agency salary costs may be reimbursed by NIST. For further information, contact:

CSD Contact:

Mr. Matthew Scholl  
(301) 975-2941  
matthew.scholl@nist.gov

ACD Contact:

Mr. Kevin Stine  
(301) 975-4483  
kevin.stine@nist.gov

### Federal Computer Security Managers' (FCSM) Forum

The FCSM Forum is covered in detail in the Outreach section of this report. Membership is free and open to federal employees. For further information, contact:

Ms. Patricia Toth

(301) 975-5140

ptoth@nist.gov or sec-forum@nist.gov

Visit the FCSM Forum website:

<http://csrc.nist.gov/groups/SMA/forum/membership.html>

### Security Research

NIST occasionally undertakes security work, primarily in the area of research, funded by other agencies. Such sponsored work is accepted by NIST when it can cost-effectively further the goals of NIST and the sponsoring institution. For further information, contact:

CSD Contact:

Mr. Matthew Scholl  
(301) 975-2941  
matthew.scholl@nist.gov

ACD Contact:

Mr. Kevin Stine  
(301) 975-4483  
kevin.stine@nist.gov

### Funding Opportunities at NIST

NIST funds industrial and academic research in a variety of ways. The Small Business Innovation Research Program funds R&D proposals from small businesses; see <http://www.nist.gov/sbir>. NIST also offers other grants to encourage work in specific fields: precision measurement, fire research, and materials science. Grants/awards supporting research at industry, academia, and other institutions are available on a competitive basis through several different Institute offices.

For general information on NIST grants programs, please contact:

Mr. Christopher Hunton

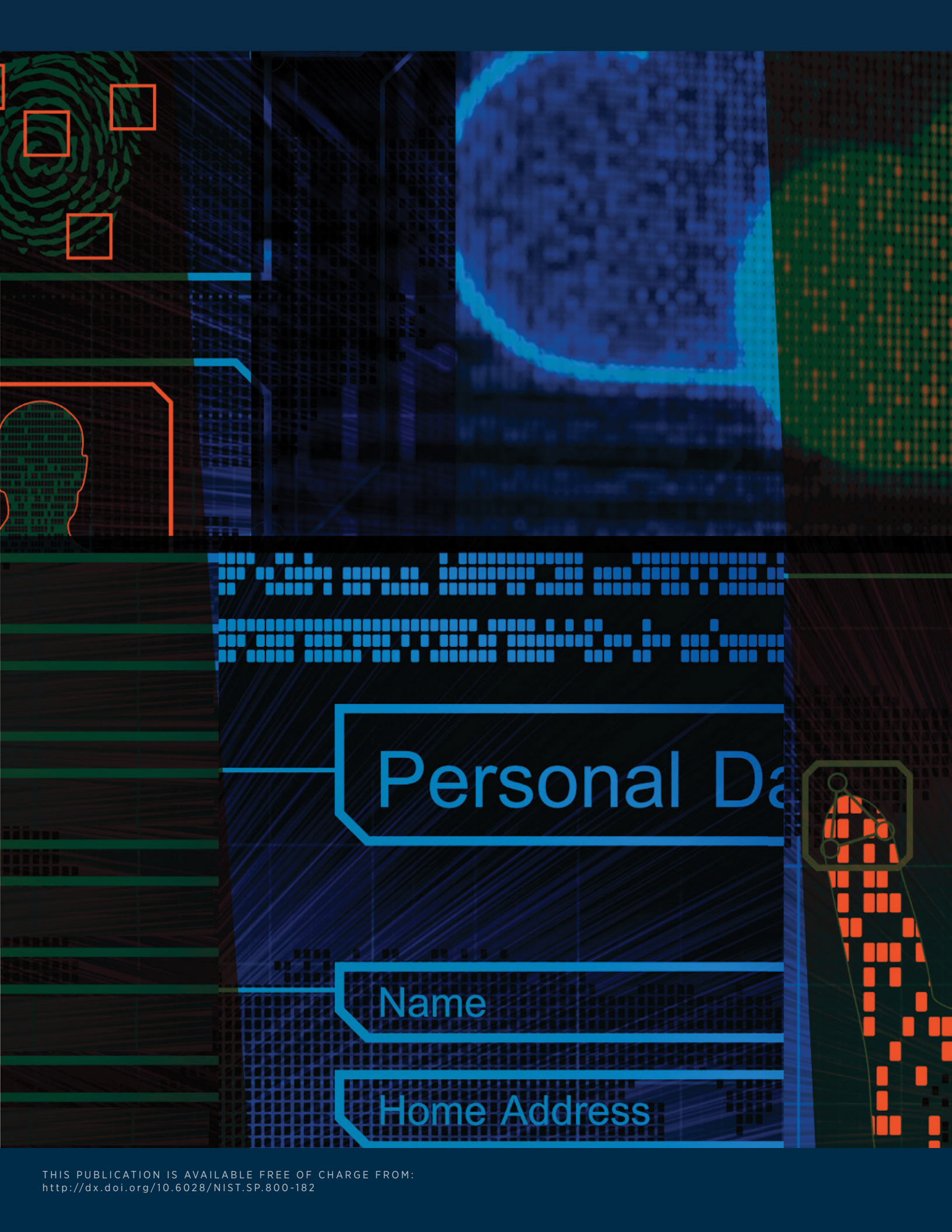
(301) 975-5718

christopher.hunton@nist.gov

Funding opportunity information:

<http://www.nist.gov/director/ocfo/grants/grants.cfm>





Personal Data

Name

Home Address