

# Overview of NIST Role in Information Assurance (IA) and Cybersecurity (CS) Standards

Jim St.Pierre  
Deputy Director  
Information Technology Laboratory  
National Institute of Standards and Technology

March 11, 2009

# Background

- ▶ The U.S. economy and U.S. citizens are heavily reliant on information technology (IT)
  - No sector today could function without IT
  - Energy, supply chain, finance, ecommerce, transportation, health care
- ▶ Although considerable progress has been made in improving cybersecurity capabilities to protect IT, there is much yet to be done
  - Determine how to mitigate new threats and secure new technologies
- ▶ Cybersecurity needs to become more standards-based to further improve quality and efficiency. Cybersecurity also needs to become easier for people to adopt and use
  - These changes would significantly reduce the cost of security implementation and management, as well as the economic impact of cybersecurity incidents

# National Priorities

## ▶ Administration Priorities

- Comprehensive National Cybersecurity Initiative (HSPD-23/NSPD-54), January 2008
- President Obama, May 2009, regarding the nation's cyber infrastructure: "Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage."
- Cyberspace Policy Review, May 2009: "The global challenge of securing cyberspace requires an increased effort in multilateral forums. This effort should seek—in continued collaboration with the private sector—to improve the security of interoperable networks through the development of global standards...."
- Science and Technology Priorities for the FY2011 Budget (August 2009)
  - "Improving and protecting our information, communication, and transportation infrastructure, which is essential to our commerce science, and security alike"

## ▶ Congressional Initiatives

- Federal Information Security Management Act of 2002
- Draft Cybersecurity Act of 2009 and other draft legislation

# Examples of Key Stakeholders

## National and International Standards Bodies



## Industry Organizations

- Smart Card Alliance
- Security Industry Association
- International Biometrics Industry Assoc.
- IPv6 Forum

## Key Industry Players

- Apple
- EMC2
- Microsoft
- Oracle
- Red Hat

## Federal Government



## Other Government Organizations

- CIO Council
- Information Security & Identity Management Committee
- Standards and Conformity Assessment Working Group

# Mandates Related to IA and CS

- ▶ Biometrics
  - USA PATRIOT Act
  - Enhanced Border Security and Visa Entry Reform Act
  - Homeland Security Presidential Directive #12: Policy for a Common Identification Standard for Federal Employees and contractors
  - 10-Print Transition: mandated by Homeland Security Council Deputies Committee
  - National Security Presidential Directive #59/ Homeland Security Presidential Directive #24: Biometrics for Identification and Screening to Enhance National Security.
- ▶ Cybersecurity
  - Federal Information Security Management Act (FISMA) of 2002 (Title III of the E-Government Act), including
    - Information Security and Privacy Advisory Board (ISPAB) mandate amended
  - Computer Security Research and Development Act of 2002
  - Homeland Security Presidential Directive #12
  - Homeland Security Presidential Directive #7: Critical Infrastructure Identification, Prioritization, and Protection
  - Conference Report on House Resolution 5441, Department of Homeland Security Appropriations Act, 2007: Title V – General Provisions (WHTI Certification effort)
  - OMB M04-04 E-Authentication Guidance for Federal Agencies
  - Information Technology Management Reform Act of 1996, Public Law 104-106
  - OMB Circular A-130 and OMB Directive 05-24
- ▶ Healthcare
  - American Recovery and Reinvestment Act
- ▶ Internet Protocol version 6 (IPv6)
  - OMB memo M-05-22 on Transition Planning for IPv6 (August 2, 2005)
- ▶ Voluntary Voting System Standards
  - Help America Vote Act

# Why NIST?

- ▶ Provides the objectivity and neutrality that are vital to success
  - Objectivity—standards are based on scientific research
  - Neutrality—standards are not designed to benefit one segment of an industry over the economic interests of another
  - Openness—standards undergo a comprehensive public review process prior to publication
- ▶ Technical source of IA and CS expertise for Federal agencies
- ▶ Long history of cooperation with U.S. industry in the development of standards
- ▶ Public and industry “buy-in” to foster widespread implementation
- ▶ Collaborative access to international cybersecurity expertise in industry, academia, and standards organizations
- ▶ National perspective vs. community-specific focus
- ▶ NIST mandated to develop cybersecurity standards

# NIST Role

- ▶ NIST is obligated by statute to develop standards and to coordinate with other agencies
  - HSPD-12, 2004: Dept. of Commerce required to develop a “Federal standard for secure and reliable forms of identification”
  - FISMA, 2002: NIST responsible “for developing standards and guidelines” for cybersecurity
  - OMB Circular A-130, 2002: “The Department of Commerce through NIST is assigned the responsibility to develop and issue security standards and guidelines...”
  - Computer Security Act, 1987: NIST responsible for developing standards and guidelines for Federal computer systems
- ▶ NIST supports IA and CS standards in several ways
  - Develop and revise standards
  - Evaluate candidates for a standard
  - Coordinate other standards efforts
  - Establish validation programs to confirm standards implementation
  - Provide guidance to agencies on how to use standards and standards-based technologies
  - Actively submit NIST-developed standards to national and international standards organizations to provide a base for harmonization of standards

# IA and CS Research and Standards (1)

## ▶ Software Assurance Metrics and Tool Evaluation (SAMATE)

- Research on metrics to assess the effectiveness of tools and techniques used for software assurance, leads to improved tools and provides assurance to users of the benefits of the tools
- Leveraging MITRE and security community work in defining a Common Weakness Enumeration (CWE) to help establish “ground truth” for tool testing

## ▶ Computer Forensics Tool Testing (CFTT) Project

- Provides metrics of assurance that the tools used by law enforcement in the investigations of computer-related crimes produce valid results
- Develop specifications for tools and establish testing methodology

58	2005-11-02	Java	Source Code	SecureSoftware	C	Not using a random initialization vector with Cipher Disk...	✗
71	2005-11-07	Java	Source Code	SecureSoftware	C	Omitting a break statement so that one may fall through is often...	✗
1050	2006-06-22	Java	Source Code	Jeff Meisler	C	Tainted input allows arbitrary files to be read and written...	✗
1050	2006-06-22	Java	Source Code	Jeff Meisler	C	Tainted input allows arbitrary files to be read and written...	✓
1054	2006-06-22	Java	Source Code	Jeff Meisler	C	Two file operations are performed on a filename, allowing a filename...	✗
1967	2006-06-22	Java	Source Code	Jeff Meisler	C	The credentials for connecting to the database are hard-coded...	✗
1968	2006-06-22	Java				The credentials for connecting to the database are...	✓
1969	2006-06-22	Java					✓
1970	2006-06-22	Java					✗
1071	2006-06-22	Java					✓
1970	2006-06-22	Java					✗



# IA and CS Research and Standards (2)

## ▶ SCAP

- Suite of specifications that standardize and help automate information classification, correlation, and sharing.
- Current use cases: vulnerability/patch management, configuration management, compliance management
- Enables security product interoperability



## ▶ NVD

- NVD is the U.S. government repository of public vulnerability management information.
- Used by government, industry and academia
- Over 40,000 CVE entries with the NVD Analysis Team evaluating over 6,000 vulnerabilities a year
- XML data feeds for SCAP reference data
- Product dictionary containing over 18,000 unique product names
- Spanish and Japanese language translations



# IA and CS Research and Standards (3)

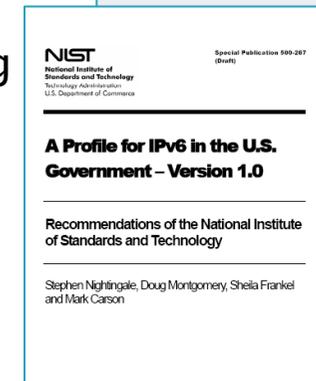
## ▶ SCRM

- Comprehensive National Cybersecurity Initiative 11: Develop Multi-Pronged Approach for Global Supply Chain Risk Management (SCRM)
- Provide US Government with robust toolset of supply chain methods and techniques
- Multi-tiered Approach:
  - Cost effective procurement related strategies
  - Industry input into supply chain practices and development of international standards
  - Ability to share supply chain incident information



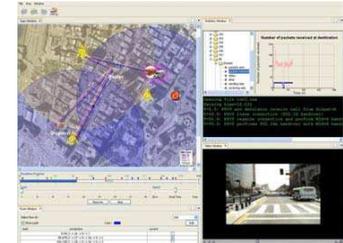
# IA and CS Research and Standards (4)

- ▶ **FISMA Implementation Project**
  - Federal Information Processing Standard (FIPS) 199 and FIPS 200 are standards that specify minimum security requirements for Federal information and information systems
  - Ongoing research and outreach efforts to keep SP 800-53, which contains the detailed requirements, up-to-date
- ▶ **Federal Desktop Core Configuration (FDCC)**
  - Standardized security configurations for operating systems and automated tools to test the configurations, improving security and saving IT security management resources
  - Implemented on millions of Federal desktop and laptop computers
- ▶ **Internet Protocol Version 6 (IPv6)**
  - Providing test and measurement tools for hardening existing Internet protocols: Standards, deployment, and testing of Internet Protocol (IPv6)
  - Published the U.S. Government IPv6 Profile, and developed strategies for conformance and interoperability testing



# IA and CS Research and Standards (5)

- ▶ **Seamless and Secure Mobility**
  - Standards and tools to provide users with ubiquitous connectivity and the ability to roam seamlessly and securely across networks of different types
  - Collaborating on IEEE 802.21 Media Independent Handover standards, IETF mobility optimization specification
- ▶ **National Software Reference Library**
  - Provides a repository of known software, file profiles, and file signatures for use by law enforcement and other organizations in computer forensics investigations
  - Published quarterly as Standards Reference Data: NIST Special Database 28



# IA and CS Research and Standards (6)

## ▶ Usability of Security

- Performing groundwork research to define factors that enable usability in the area of multifactor authentication and developing a framework for determining metrics that are critical to the success of usability

## ▶ Identity Management Systems

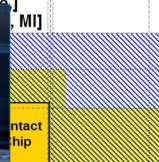
- Standards development work in biometrics, smart cards, identity management, and privacy framework.
- R&D: Personal Identity Verification, Match-On-Card, ontology for identity credentials, development of a workbench
- ID Credential Interoperability



© Pato Zvonar | Dreamstime.com



© Graeme Dawes | Dreamstime.com



# IA and CS Research and Standards (7)

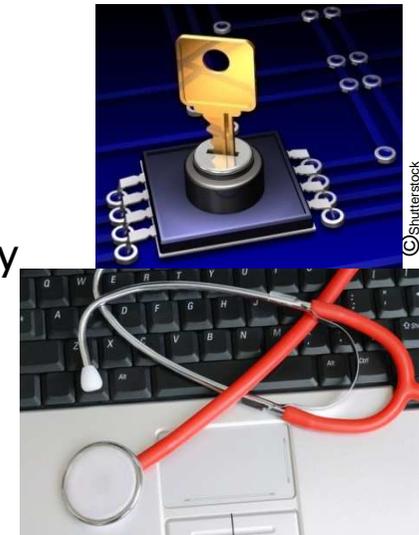
## ▶ Smart grid security

- Coordinate development of cybersecurity elements of a framework of protocols and model standards; continuously coordinated with networking standards and guidance
- Selecting use cases from existing sources, e.g., IntelliGrid, Electric Power Research Institute (EPRI), and Southern California Edison (SCE)
- Use cases provide a common framework for performing the risk assessment, developing the security architecture, and selecting and tailoring the security requirements



## ▶ Healthcare information technology

- NIST provides security specifications for enabling communicating parties to transmit health information securely and to ensure privacy and confidentiality
- Developing guidelines for HIPAA Security Rule and Security Architecture Design Process for Health Information Exchanges
- Leveraging prior cybersecurity efforts



© Shutterstock

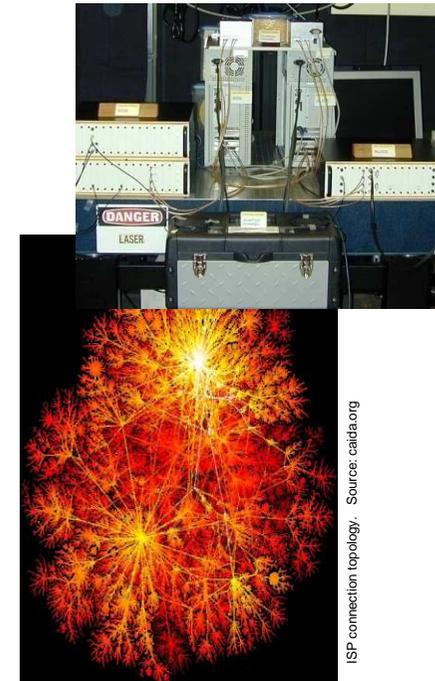
© Andrzej Tokarski | Dreamsstime.com

**NIST**

National Institute of Standards and Technology

# IA and CS Research and Standards (8)

- ▶ Foundations of Measurement Science for Information Systems
  - Large-scale systems (e.g., the Internet, power grid) deployed without fundamental understanding of their range of behaviors, security; Information systems lack same foundations as physical sciences
  - Basic research program: mathematical foundations underlying development of a measurement science for information systems; Initial Focus: Abstract models of information systems structure, dynamics



# Improving IA and CS Through Standards and Testing —Success Stories

- ▶ **Advanced Encryption Standard (AES)**
  - Protects sensitive data being stored or transmitted
  - Adopted voluntarily by national and international standards organizations
  - Incorporated at minimum cost and without royalty fees
- ▶ **SCAP Validation Program**
  - Ensures interoperability between products
  - 32 products from 24 vendors currently validated
- ▶ **Multifactor Authentication**
  - Developing standards for biometrics, smart card interfaces, and entity authentication
  - Working with vendors, other federal agencies, and the international community

# Moving Forward

- ▶ Continue ongoing standards development efforts
- ▶ Technical leadership and coordination in support of guidelines, standards and testing efforts, including:
  - SCAP
    - Remediation capabilities
    - Expanding to support more operating systems and applications
  - SCRM
    - NIST Inter–Agency Report (NISTIR) 7622 *Piloting Supply Chain Risk Management Practices for Federal Information Systems*
      - Publish: April, 2010
    - Future NIST Special Publication
      - First Public Draft: Winter, 2011
    - ISO CS–1 Global Supply Chain Risk Management Ad Hoc Working Group

# Moving Forward (2)

- ▶ Technical leadership and coordination in support of guidelines, standards and testing efforts, including:
  - NVD
    - Expand data and search capabilities to include configuration settings via Common Configuration Enumeration (CCE)
    - Expand data feeds to include 800–53 control mappings for a wide range of operating systems and applications, supporting compliance reporting
  - SAMATE
    - Develop additional test suites for assessing the effectiveness of web application scanner tools
    - Investigate additional problems in static source code analysis during annual Static Analysis Tool Exposition (SATE)
    - Improve utility of SAMATE Reference Dataset through:
      - Guidance in running tools against SRD test cases
      - Establish quality levels of tests used in tool effectiveness assessment
      - Broaden the SAMATE Reference Dataset (SRD) repository test content in areas of test language and size and tool application

