NIST’s Computer Security Program

A Review of Activities and a Look Ahead

Donna F Dodson

Division Chief, Computer Security Division

Deputy Cyber Security Advsor

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 cyber security capabilities to protect IT, there is much yet to be done
  - Determine how to mitigate new threats and secure new technologies
- Cyber security 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 Cyber security 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

Mandates Related to Cybersecurity

- 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.
- Cyber security
  - 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

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 cyber security
  - 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 cyber security 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

Computer Security Division 893

Core Focus Area

- Research, Development, and Specification
  - Security Mechanisms (e.g. protocols, cryptographic, access control, auditing/logging)
  - Security Mechanism Applications
    - Confidentiality
    - Integrity
    - Availability
    - Authentication
    - Non-Repudiation
- Secure System and Component configuration
- Assessment and assurance of security properties of products and systems

NIST Work in Cyber Security

- FISMA Phase II
  - Continue to support the Joint Task Force Transformation Initiative (DoD, IC, NIST, CNSS) and support unified information security framework
  - Continue support for risk management and information security publications
  - Potential privacy and threat appendixes for SP 800-53, Revision 3
  - Work toward system and security engineering and application security guidelines
- US Government Configuration Baseline (USGCB)
  - Standardized security configurations for operating systems and automated tools to test the configurations, improving security and saving IT security management resources
- Security Automation and Vulnerability Management
  - Continue to develop tools and specifications that address situational awareness, conformity and vulnerability management compliance etc

FIPS PUB 199

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Standards for Security Categorization of Federal Information and Information Systems

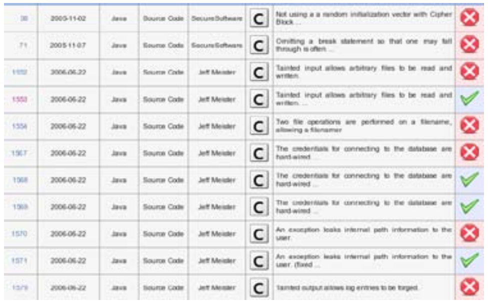
FIPS PUB 200

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

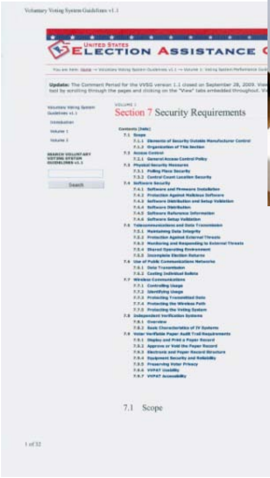
Minimum Security Requirements for Federal Information and Information Systems

NIST Work in Cyber Security

- Virtualization and Cloud
  - Support for cloud special publication and standards activities to support security, portability and interoperability
- Key Management
  - Foster the requirements of large-scale key management frameworks and designing key management systems
  - Support transitioning of cryptographic algorithms and key sizes
- Next Generation Cryptography
  - Open competition for new Hash algorithm
  - Developing new, light weight, quantum resistant encryption for use in current and new technologies
  - New modes of operation



38	2005-11-02	Java	Source Code	SecureSoftware	C	Not using a a random initialization vector with Cipher Block ...	☒
71	2005-11-07	Java	Source Code	SecureSoftware	C	Omitting a break statement so that one may fall through is often ...	☒
1552	2006-06-22	Java	Source Code	Jeff Meister	C	Tainted input allows arbitrary files to be read and written.	☒
1553	2006-06-22	Java	Source Code	Jeff Meister	C	Tainted input allows arbitrary files to be read and written. ...	✓
1554	2006-06-22	Java	Source Code	Jeff Meister	C	Two file operations are performed on a filename, allowing a filenamer	☒
1567	2006-06-22	Java	Source Code	Jeff Meister	C	The credentials for connecting to the database are hard-wired ...	☒
1568	2006-06-22	Java	Source Code	Jeff Meister	C	The credentials for connecting to the database are hard-wired ...	✓
1569	2006-06-22	Java	Source Code	Jeff Meister	C	The credentials for connecting to the database are hard-wired ...	✓
1570	2006-06-22	Java	Source Code	Jeff Meister	C	An exception leaks internal path information to the user.	☒
1571	2006-06-22	Java	Source Code	Jeff Meister	C	An exception leaks internal path information to the user. (fixed ...	✓
1579	2006-06-22	Java	Source Code	Jeff Meister	C	Tainted output allows log entries to be forged.	☒



Voluntary Voting System Guidelines v1.1

UNITED STATES ELECTION ASSISTANCE C

You are here: Home → Voluntary Voting System Guidelines v1.1 → Volume 1: Voting System Performance Guid

Update: The Comment Period for the VVSG version 1.1 closed on September 28, 2009. View
tool by scrolling through the pages and clicking on the "View" tabs embedded throughout. Vi

Voluntary Voting System Guidelines v1.1

Introduction

Volume 1

Volume 2

SEARCH VOLUNTARY VOTING SYSTEM GUIDELINES v1.1

Search

VOLUME 1

Section 7 Security Requirements

Contents [hide]

- 7.1 Scope
  - 7.1.1 Elements of Security Outside Manufacturer Control
  - 7.1.2 Organization of This Section
- 7.2 Access Control
  - 7.2.1 General Access Control Policy
- 7.3 Physical Security Measures
  - 7.3.1 Polling Place Security
  - 7.3.2 Central Count Location Security
- 7.4 Software Security
  - 7.4.1 Software and Firmware Installation
  - 7.4.2 Protection Against Malicious Software
  - 7.4.3 Software Distribution and Setup Validation
  - 7.4.4 Software Distribution
  - 7.4.5 Software Reference Information
  - 7.4.6 Software Setup Validation
- 7.5 Telecommunications and Data Transmission
  - 7.5.1 Maintaining Data Integrity
  - 7.5.2 Protection Against External Threats
  - 7.5.3 Monitoring and Responding to External Threats
  - 7.5.4 Shared Operating Environment
  - 7.5.5 Incomplete Election Returns
- 7.6 Use of Public Communications Networks
  - 7.6.1 Data Transmission
  - 7.6.2 Casting Individual Ballots
- 7.7 Wireless Communications
  - 7.7.1 Controlling Usage
  - 7.7.2 Identifying Usage
  - 7.7.3 Protecting Transmitted Data
  - 7.7.4 Protecting the Wireless Path
  - 7.7.5 Protecting the Voting System
- 7.8 Independent Verification Systems
  - 7.8.1 Overview
  - 7.8.2 Basic Characteristics of IV Systems
- 7.9 Voter Verifiable Paper Audit Trail Requirements
  - 7.9.1 Display and Print a Paper Record
  - 7.9.2 Approve or Void the Paper Record
  - 7.9.3 Electronic and Paper Record Structure
  - 7.9.4 Equipment Security and Reliability
  - 7.9.5 Preserving Voter Privacy
  - 7.9.6 VVPAT Usability
  - 7.9.7 VVPAT Accessibility

7.1 Scope

Return to Top

1 of 32

10/6/2009 3:52 P

© Lisa F. Young/Dreamstime.com

NIST
National Institute of Standards and Technology

NIST Work in Cyber Security

- 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
- Infrastructure support
  - Continued support for Health IT, Smart Grid and Voting
- Standards Development Organizations

◦ IETF	ANSI
◦ IEEE	ISO

© Peto Zvonar | Dreamstime.com

© Graeme Dawes | Dreamstime.com

National Institute of Standards and Technology

For Additional Information

- NIST's Information Technology Lab
  - http://www.itl.nist.gov/
- Computer Security Resource Center
  - http://csrc.nist.gov
- National Vulnerability Database
  - http://nvd.nist.gov
- Biometrics Resource Center
  - http://www.itl.nist.gov/div893/biometrics
- NIST
  - http://www.nist.gov/
- Biometrics Research
  - Finger: http://fingerprint.nist.gov
  - Face: http://face.nist.gov
  - Iris: http://iris.nist.gov