

Documentary Standards Update: Cybersecurity

NIST VCAT
June 8-9 2010

Cybersecurity: Major Accomplishments

▶ Cryptography

- ▶ Cryptographic Mode for Secure Disk Drives published
- ▶ Revised Key Exchange offers enhanced interoperability for IPv6/IPsec implementations
- ▶ Support for NIST-Approved Cryptographic algorithms increased in IETF specifications

▶ Biometrics

- ▶ NIST-edited ISO/IEC standards for testing fingerprint data, match on card performance, and biometric fusion reach International Standard

▶ FISMA

- ▶ Enhancing alignment of ISO/IEC 27000-series with FISMA specifications

Cybersecurity: Major Accomplishments

- ▶ **Identity Management Systems**
 - ▶ Personal Identification Verification specifications updated to additional key management properties and cryptographic algorithm interoperability
 - ▶ ISO/IEC Smart Card Standards moving to Final Draft International Standard
- ▶ **Security Automation and Vulnerability Management**
 - ▶ New U.S. Government Configuration Baseline specifications
- ▶ **Enhancing Security and Stability of the Internet**
 - ▶ Deployment in the Root Zone simplifies configuration and promotes adoption of DNSSEC (signed root zone to be operational in July 2010)

Cybersecurity: Challenges and Opportunities

- ▶ Aligning FISMA and the ISO/IEC 27000-series
- ▶ Many aspects of Clouds, many SDOs
- ▶ Securing the “Internet of Things”
- ▶ Managing standardization strategy for Security Content Automation Protocol
- ▶ Internet Infrastructure Protection standards
- ▶ Usability for {Biometrics, Cryptography, ... }

Cybersecurity: Current Events

▶ Upcoming Events

- ▶ ANSI/NIST-ITL Standard Workshop: Interchange of Fingerprint, Facial, & Other Biometric Information (July 2010)
- ▶ Second SHA-3 Candidate Conference (August 2010)
- ▶ 6th Annual IT Security Automation Conference (September 2010)

▶ Recent Events of Interest

- ▶ International Biometric Performance Conference (March 2010)
- ▶ Cloud Computing Forum and Workshop (May 2010)