

INCITS/CS1 (Cyber Security) Liaison Report to T11

Eric A. Hibbard, CISSP, CISA
June 4, 2009

Organizational Info

◆ Officers

- CS1 Chair – Dan Benigni (NIST)
- CS1 IR – Eric Hibbard (HDS)
- CS1 Secretary – Laura Kuiper (Cisco)
- CS1.1 TG Chair – Ed Coyne (SAIC)

◆ CS1 Technical Committee Structure

- CS1.1 Task Group
- Ad Hoc - SOBISH
- Ad Hoc - ISMS (27001/27002)
- Ad Hoc - Policy Machine
- Ad Hoc on ID Assurance
- Ad Hoc on Supply Chain Risk Management

Domestic Activities

- ◆ ANSI INCITS 359–2004 Role-based Access Control
 - INCITS re-affirmed INCITS 359:2004 [R2009]
 - CS1 also approved an INCITS Project Proposal for the Revision of INCITS 359:2004 (INCITS Project 1544-M)
- ◆ INCITS Project 1794-D:
 - Title: *Requirements for the Implementation and Interoperability of Role Based Access Control (RBAC)*
 - CS1 Letter Ballot completed; revised draft produced.
- ◆ INCITS Project 2148-D:
 - Title: *Small Organization Baseline Information Security Handbook (SOBISH)*
 - Coordinating work with NIST, which plans to publish a security guide for small businesses
 - Focus is still small and mediums sized organizations and to provide comprehensive security guidance (including compliance) that is aligned with ISO/IEC 27001/27002

International Activities

- ◆ SC27 Organizational Structure:
 - WG 1 – Information security management systems
 - WG 2 – Cryptography and security mechanisms
 - WG 3 – Security evaluation criteria
 - WG 4 – Security controls and services
 - WG 5 – Identity management and privacy technologies
- ◆ Preparing the U.S. comments and positions on several drafts and NWIs.
 - Special attention is begin given to the revision of ISO/IEC 27001 & 27002
 - See backup slides for more details
- ◆ Early preparations for the next ISO/IEC JTC SC27 meeting, which is being hosted by the U.S. (Redmond, WA)
- ◆ Preparing for output documents from the Beijing meeting

Meeting Information

- ◆ INCITS TC CS1 Cyber Security:
 - F2F: Aug 19-20, 2009; Vancouver, BC
 - F2F: Sep 30 – Oct 1, 2009; Pittsburgh, PA
 - F2F: Jan 13-14, 2010; Washington, DC (Tentative)
 - F2F: Feb 24-25, 2010; Santa Clara, CA (Tentative)
- ◆ INCITS TG CS1.1
 - F2F: July 14, 2009; Washington, DC
- ◆ ISO/IEC SC 27 (Security Techniques):
 - Last WGs & Plenary: May 4-8, 2009; Beijing, China
 - WGs: Nov 2-6, 2009; Seattle, WA (U.S. hosting)
 - WGs & Plenary: Apr 19-27, 2010; Melaka, Malaysia
 - WGs: Oct/Nov, 2010; Europe
 - WGs & Plenary: Apr/May, 2011; Singapore

Backup Slides

09-333v0

ISO/IEC SC27 Important Projects

- ◆ ISO/IEC 27000:2009 Information security management systems - Overview and vocabulary
- ◆ ISO/IEC 27001 Specification for an ISMS (WD)
- ◆ ISO/IEC 27002 Code of practice for Information Security Management (WD)
- ◆ ISO/IEC 27003 Information security management system implementation guidance (register and circulate as FDIS)
- ◆ ISO/IEC 27004 Information security management measurements (register and circulate as FDIS)
- ◆ ISO/IEC 27007 Guidelines for ISMS auditing (register and circulate as CD)
- ◆ ISO/IEC TR 27008 Guidance for Auditors on ISMS Controls (circulate as 3rd WD)
- ◆ ISO/IEC 27031 Specification for ICT Readiness for Business Continuity (register and circulate as CD)

ISO/IEC SC27 Important Projects (cont.)

- ◆ ISO/IEC 27032 Guidelines for Cybersecurity
- ◆ ISO/IEC 27033 IT network security (multi-part)
 - Part 1 – Overview and concepts (FCD)
 - Part 2 – Application security management process (CD)
- ◆ ISO/IEC 27034 Application security (CD)
- ◆ ISO/IEC 27035 Security incident management (circulate as FCD)
- ◆ ISO/IEC 29000 Privacy Framework (register and circulate as CD)
- ◆ ISO/IEC 29001 Privacy Reference Architecture (circulate as 3rd WD)

ISO/IEC SC27 Other Projects of Possible Interest

- ◆ ISO/IEC 27009: Guidance for auditors on ISMS controls.
- ◆ ISO/IEC 27010: Information security management for inter-sector communications (WD)
- ◆ ISO/IEC 27035: Information security incident management (CD).
- ◆ ISO/IEC 29128: Verification of cryptographic protocols (CD)
- ◆ ISO/IEC 29146: A framework for access management (WD)
- ◆ ISO/IEC 29147: Responsible vulnerability disclosure (3rdWD)
- ◆ ISO/IEC 29149: Best practice on the provision of time-stamping services (4thWD)
- ◆ ISO/IEC 29150: Signcryption (CD)

ISO/IEC SC27 Study Period Topics

- ◆ Access control
- ◆ Secret sharing mechanisms
- ◆ Mechanisms supporting anonymity
- ◆ Tamper protection requirements and evaluation
- ◆ Redaction