INCITS/CS1 (Cyber Security) Liaison Report to INCITS/T11

Eric A. Hibbard, CISSP, CITP, CISA
T11-2020-00148-v000
June 4, 2020
INCITS/CS1 Organizational Info

- Officers
  - CS1 Chair – Eric Hibbard (PrivSec Consulting LLC)
  - CS1 Vice Chair – John Britton (Google)
  - CS1 IR – Nadya Bartol (BCG Platinion)
  - CS1 Secretary – Vacant

- CS1 Technical Committee Structure
  - Ad Hoc – 27RAHG
  - Ad Hoc - Application Security
  - Ad Hoc - Cybersecurity Framework
  - Ad Hoc - Datasecurity
  - Ad Hoc - Info Assurance Standards & Technology
  - Ad Hoc - IoT Security & Privacy
  - Ad Hoc - Next Generation Access Control (NGAC)
  - Ad Hoc - Privacy
  - Ad Hoc - Storage & Evidence (storage_evidence@standards.incits.org)
  - Ad Hoc - USNB Hosting SC 27
Observations/Comments

• SC 27 Name Change
  – Old: IT – Security techniques
  – New: Information security, cybersecurity, and privacy protection

• SC 27 Leadership Undergone Changes
  – Andreas Wolf (DIN) as SC 27 Chair
  – Laura Lindsay (US) as SC 27 Vice Chair
  – Committee Manager is retiring this year

• Last SC 27 meeting (April) was held via Zoom sessions
• September meeting will be held via Zoom meetings
• USNB will host the spring 2023 meeting
T11 Relationship with CS1

- CS1 is happy to continue the liaison relationship with T11
- Eric Hibbard (eric.Hibbard@gmail.com) is no longer employed by a T11 member; can continue to represent CS1
- CS1 is interested in security/privacy activities in T11
- Except for an ANSI RBAC standard, all of CS1’s activities are international (SC 27), but this could change in the future
ISO/IEC 27040 (STORAGE SECURITY)
Background

• U.S. Proposed Early Revision of ISO/IEC 27040:2015
  – SC 27 conducted 6-month Study Period
  – Study Period explored multi-part scenario and other issues
    • Recommended starting with single part with provisions for multi-part
    • Change from guidance to requirements/guidance
• Due to scope change, 27040 revision was balloted as a new work item proposal (NWIP)
  – NWIP ballot passed
  – Several comments submitted on the preliminary draft
• Expanded editing team
  – Project Editor: Eric Hibbard
  – Co-Editors from CN and FR
Initial Changes

• Title Change: *Information technology – Storage security*

• Scope Change:
  – Original scope preserved, but “guidance” statements changed to “requirements and guidance”
  – CN commented that 27040 should be expanded to cover *storage trustworthiness* and to cover *development* (i.e., what applies to vendors); *rejected* due to lack of contributions, but they will be back

• Preliminary Draft:
  – Based on the published standard
  – Contained a small number of requirements
  – Fixed a few known problems (e.g., added data protection sub-clause)
ISO/IEC WD 27040.1

- Structure Changes (moderate):
  - Cloud moved out of Object Storage into its own sub-clause
  - Hardening under storage management moved into a new sub-clause on system security
- All requirements currently in Clause 6 (Supporting Controls);
- Clause 7 (Guidelines for the design and implementation of storage security) is fair game
- Sanitization
  - Storage with sensitive data shall only be disposed of after being sanitized (paraphrased)
  - Annex A (Media sanitization) is targeted for removal
  - Descriptive language moved to Annex C
  - 27040 expected to defer the media-specific details to IEEE P2883 (Standard for Sanitizing Storage)
ISO/IEC WD 27040.1 (cont.)

• Items under consideration for removal:
  – Fibre Channel over Ethernet (FCoE)
  – Parallel NFS (pNFS)
  – SCSI Object-based Storage Device (OSD)
  – Content Addressable Storage (CAS)

• Items under consideration for additions:
  – Generic object-based storage
  – Security details for NVMe-oF
  – Software Defined Storage (SDS)
  – Persistent memory (e.g., NVDIMM-P and NVDIMM-N)

• Undecided:
  – FC-SP-2 (especially link encryption)
How to Get Involved

• 27040 WD ballot closes 2020-07-24
• Expert-level input, so CS1 not likely to engage until CD
• SNIA (Security TWG) and IEEE SISWG actively discussing and preparing contributions; materials will be submitted under the IEEE Computer Society Cat A liaison to SC 27
• Contact eric.hibbard@gmail.com