IDS Face-to-Face Minutes
February 9, 2023

Meeting was called to order at approximately 10:00 am ET February 9, 2023.

Attendees –

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Smith Kennedy	HP Inc.
Jeremy Leber	Lexmark
Ira McDonald	High North
Anthony Suarez	Kyocera
Alan Sukert	
Michael Sweet	Lakeside Robotics
Bill Wagner	TIC

Agenda Items

Note: Meeting slides are available at https://ftp.pwg.org/pub/pwg/ids/Presentation/2023-02-09-IDS-F2F v1.pdf.

- Minute Taker
  - Alan Sukert taking the minutes.

2. Agenda:
   - Introductions, Agenda Review
   - Discuss status of the Hardcopy Device international Technical Community (HCD iTC) Meetings and the HCD collaborative Protection Profile (cPP)/Supporting Document (SD) since the publishing of v1.0
   - Special Topic on Cybersecurity in the US
   - HCD Security Guidelines v1.0 Status
   - Trusted Computing Group (TCG) / Internet Engineering Task Force (IETF) Liaison Reports
   - Wrap-Up / Next Steps
3. Alan went quickly through the PWG Antitrust, Intellectual Property and Patent policies.
4. Alan went through the current status of the HCD iTC and the status of the HCD cPP v1.0 and HCD SD v1.0 since the two documents were published on Oct 31, 2022. Some of the key points from this discussion were:

   - The HCD iTC is currently awaiting Position Statements from NIAP (US), ITSCC (Korea), JISEC (Japan) and the Canadian Scheme. NIAP indicated they are currently reviewing the HCD cPP, so we may get a Position Statement from NIAP soon. However, we haven't heard any status from either ITSCC or JISEC.

     The Canadian Scheme did indicate that it may have a vendor that wants to certify an HCD against the published HCD cPP / HCD SD as soon as possible, so that may hasten its review of the two documents and issuance of its Position Statement.

     At the International Common Criteria Conference during his talk Al was asked if there was a document that indicated that changes in the HCD cPP from the HCD PP. Al put together two documents that indicate the major changes of the HCD cPP and HCD SD, respectively, from the HCD PP; these documents are posted on the HCD iTC OnlyOffice site.

   - Al then gave the status of the HCD Interpretation Team.as follows:

     - The HIT currently has 7 members. The goal is to have a maximum of 10 members on the HIT, but 7 is a good number to start with. We have designated a HIT Lead (Al) and a HIT

Deputy Lead (Jerry Colunga). The current membership is from HCD vendors and an Evaluation Lab, although NIAP may provide a member which would be a very good thing.

- HIT procedures under development. Al is working on the final draft which he hoped to have by Friday, but will more likely be ready for HIT member review on Monday Feb 13th. The big thing is that the HIT will be the first Interpretation Team to using GitHub for documenting and processing Requests for Interpretation (RfIs) and for creating and tracking changes to HCD cPP v1.0 and HCD SD v1.0 for approval of RFIs. Al is working on adding the GitHub processing into the HIT procedures – Slide 9 shows where GitHub fits into the overall RFI general process.
- The HIT will be responsible for maintaining the Interpretation baseline while the Editors will be responsible for maintaining the Master baseline. The HIT will actually have to maintain two baselines for approved RfIs that require changes to either the HCD cPP v1.0 or HCD SD v1.0:
  - One baseline for the approved changes to either document that are also approved by NIAP as NIAP Technical Decisions (TDs)
  - One baseline for the approved changes to either document that are not approved by NIAP
- Finally, we are looking to have the HIT fully implemented by the end of February 2023. The fact that the Canadian Scheme may have a certification against v1,0 soon is certainly pushing this to happen.

In the HIT discussion Ira mentioned the fact that we can expect the number of RfIs that the HIT will see will increase as more HCDs start getting certified against the new HCD cPP and HCD SD. We've added some new SFRs like Secure Boot that have not been in any cPPs before, so it is reasonable to expect will see a lot of questions and issues against the new cPP and SD.

- Slides 10 and 11 showed the current Parking Lot issues. The list has not changed from the list shown at the November IDS Face-to-Face Session. What has changes is the importance of some pf the Parking Lot issues, especially the ones related to TLS 1.3 and removal of support for TLS 1.1, SHA-1 support, cipher suites with RSA Key Generation with keys < 2048 bits and all RSA and DHE Key Exchanges.
- The one issue the HCD iTC is working on now is a release plan for v1.1 and future releases of the HCD cPP and HCD SD. We have talked to other iTCs about what their release strategy is, and they have told us that basically they have no specific rules for the timeframe of their releases. A couple of things the HCD iTC has agreed on:
  - We will have major and minor releases
  - The first update to the HCD cPP and HCD SD will likely be "Errata" releases because AL did find minor editorial issues in both documents, and others probably did also

  The rest of the questions about the HCD iTC release planning are described in Slide 12.
- Al then went into a discussion of CNSA 2.0, which is one of the biggest issues the HCD iTC will have to address in v1.1 and future releases. CNSA (Commercial National Security Algorithm) 2.0 was released by NSA in Sep 2022 to address the problem that future deployment of a cryptanalytically relevant quantum computer (CRQC) would break public-key systems still used today. So, NSA needed to plan, prepare, and budget for an effective transition to quantum-resistant (QR) algorithms to assure continued protection of National Security Systems (NSS) and related assets.

  CNSA 2.0 is an update to CNSA 1.0 Algorithms and applies to all NSS use of public cryptographic algorithms (as opposed to algorithms NSA developed), including those on all unclassified and classified NSS

  The CNSA 1.0 algorithms that are currently in use by just about everyone, and which are included in the various crypto SFRs in the HCD cPP v1.0, are:

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher used for information protection	FIPS Pub 197	Use 256 bit keys to protect up to TOP SECRET
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A	Use Curve P-384 to protect up to TOP SECRET.
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384 to protect up to TOP SECRET.
Secure Hash Algorithm (SHA)	Algorithm used for computing a condensed representation of information	FIPS Pub 180-4	Use SHA-384 to protect up to TOP SECRET.
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for key establishment	NIST SP 800-56B rev 1	Minimum 3072-bit modulus to protect up to TOP SECRET
RSA	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4	Minimum 3072 bit-modulus to protect up to TOP SECRET.

The proposed CNSA 2.0 algorithms are:

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels

Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels SHA256/192 recommended
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels

The NSA transition plan for CNSA 2.0 is:

- The timing of the transition depends on the proliferation of standards-based implementations
- NSA expects the transition to QR algorithms for NSS to be complete by 2035
- NSA urges vendors and NSS owners and operators to make every effort to meet this deadline or even sooner if possible
- Where feasible, NSS owners and operators will be required to prefer CNSA 2.0 algorithms when configuring systems during the transition period.
- When appropriate, use of CNSA 2.0 algorithms will be mandatory in classes of commercial products within NSS, while reserving the option to allow other algorithms in specialized use cases

NIAP's transition plan for CNSA 2.0 is:

- Currently all NIAP PPs must have CNSA 1.0 algorithms (which they do)
- Will add SHA-512 to all NIAP PPs (Note: That is all NIAP developed PPs that must be met for the applicable products to be included in the NIAP Product Compliant List; **that does not refer to any cPPs developed by an iTC**)
- Will require either CNSA 1.0 or CNSA 2.0 be mandatory on all NIAP PPs at some point, but NIAP current has no date set for this to occur
- Will implement CNSA asymmetric algorithms for software/firmware signing per following
  - LMS – 1H 2023
  - XMSS – 2H 2023

  Note: NIAP indicated these dates likely won't be met, but digital signing for software upgrade is NIAPs #1 priority for implementation of CNSA 2.0
- Will implement following Key Establishment CNSA 2.0 algorithms in all NIAP PPs when they are standardized and all relevant Assurance Activities (and have been include in CAVP) have been defined and agreed upon:
  - CRYSTALS - Kyber
  - CRYSTALS – Dilithium (used for Digital Signatures)
- Will deprecate CNSA 1.0 in 2030 – 2033 timeframe
- **No current timeline established to make CNSA 2.0 mandatory**
- Will make use of CNSA 2.0 mandatory to be listed on PCL at some point (but again no timeframe for this to occur has been established yet)
- Will work with vendors to help try to meet NSA schedule
- Will discuss with CCRA and engage with iTCs how best to integrate CNSA 2.0 into cPPs. NIP plans to start these discussions soon.

CNSA 2.0 will be a major issue that the HCD iTC will have to face for several years and several versions of the HCD cPP/SD and we try to implement the various CNSA 2.0 algorithms into the two documents.

- Al then reviewed the likely content (in his view) for HCD cPP/SD v1.1. At the top of the list are:
  - Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
  - Inclusion of NTP
  - Inclusion of AVA_VAN and ALC_FLR.* to be consistent with EUCC and with ND cPP v3.0 since it Is included in the ND cPP v3.0 version currently in final review
  - Initial implementation of CNSA 2.0 algorithms –inclusion of SHA-384 and SHA-512 and inclusion of LMS as an option are most likely the first steps
  - Sync with ND cPP/SD v3.0 to be published sometime in 1Q 2023
  - Incorporate the NIAP SSH Package that is included in ND cPP/SD v3.0

  Some other like candidates to v1.1 are:
  - Comparisons of HCD cPP / HCD SD with ND cPP / ND SD v3.0 counterparts that AL did reveal other changes that should be looked at by the HCD iTC for inclusion
  - Changes due to any approved RfIs to HCD cPP/SD v1.0 (Note: We will have to decide if only include changes approved by NIAP)
  - Updates to CC2022 published in November 2022 – A comparison of CC2022 Part 2 to CC v3.1R5 SFRs done by Al revealed several changes that should be looked at by the HCD iTC for inclusion
  - Changes due to requests from JISEC, ITSCC or NIAP (Canada also?)
- Some changes that could go in v1.1 or future releases are:
  - Full implementation of CNSA 2.0 (that is probably #1 on this list)
  - Support for new crypto algorithms
  - NIAP IPsec Package that is under development
  - Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, NIAP TDs – this item hit home when it was just announced this week that FIPS had updated FIPS 186-5(and sunset FIPS 186-4) and NIST had selected Ascon for the Lightweight Crypto Algorithm, which means that we will now have to support EDDSA for digital signatures in the cPP. Ira mentioned that NIST has also updated SP 800-186 because of the Ascon announcement.
  - Expand to address 3D printing -this is an important future item given the increasing use of 3D printers in the public sector
  - Support for Wi-Fi and maybe Bluetooth
  - Support for Security Information and Event Monitoring (SIEM) and related systems
  - Any new CCDB Crypto WG or CCUF Crypto WG Packages
  - Support for SNMPv3
  - Support for NFC
  - Indirect updates based on new technologies or customer requests
- Next steps for the HCD iTC are:
  - Implement the HIT for maintaining HCD cPP/SD v1.0
  - Agree on the HCD cPP/HCD SD release plan
  - Determine the content for and then create the next HCD cPP/SD release (Errata and then v1.1)

- Ensure that the HCD iTC continues to be fully engaged now that HCD cPP v1.0 and HCD SD v1.0 have been published

- The final set of "Lessons Learned" from the development pf HCD cPP/SD v1.0 are:
  - It requires a dedicated group of editors to get a cPP or SD version published
  - We were lax (and that is putting it politely) in creating and monitoring our Work Plan for the HCD cPP/SD v1.0 development; need to do better for future versions of these documents
  - Work Plans and schedules need to be realistic. Ira pointed out Work Plans are never realistic, but Al stated our original plans were so unrealistic to be almost nonsensical.
  - Tracking the changes for v1.0 was a tedious manual process (Al did all of it so he says that) – it needs to be more automated for future releases (which is one of the benefits of going to GitHub for the HIT)

5. Al then went through his special topic on Cybersecurity in the US. He originally was going to do a comparison of US vs. EU cybersecurity, but it got so big he decided to focus just on cybersecurity in the US,

   He started with the following General Observations:

   - Current cybersecurity activities with the US Government are based on four key sources – the Federal Information Security Modernization Act of 2014 (or FISMA), the Cybersecurity Enactment Act of 2014, the Cybersecurity Enactment Act of 2015 and the 2021 Executive Order on Improving the Nation's Cybersecurity. There are other laws that update or expand on these four laws.
   - Cybersecurity laws apply only to what the government agencies must do; the agencies like NIST are chartered to provide standards and guidelines to implement the cybersecurity laws. This is in contrast to the EU, where the cybersecurity laws generally apply to everyone, not just to the member states.
   - US Government cybersecurity activities are spread over multiple government agencies, but primarily to NIST, CISA and DHS
   - There are a large number of cybersecurity frameworks developed by and for US Government Agencies and cybersecurity frameworks developed for specific industries or industry groups – many more than Al realized when he started this activity.

   Regarding FISMA, its main purposes are to:

   - Codify the Department of Homeland Security's role in administering the implementation of information security policies for federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting OMB in developing those policies
   - Provide the Department authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistent with OMB policies and practices
   - Authorize DHS to provide operational and technical assistance to other federal Executive Branch civilian agencies at the agency's request
   - Places the federal information security incident center within DHS by law
   - Authorize DHS technology deployments to other agencies' networks (upon those agencies' request)
   - Direct OMB to revise policies regarding notification of individuals affected by federal agency data breaches
   - Require agencies to report major information security incidents as well as data breaches to Congress as they occur and annually

   We have talked about the Cybersecurity Executive Order of 2021 in detail at a previous IDS Face-to-Face and an IDS WG Meeting, but as a reminder, the key areas covered by the Executive Order are:

- Remove Barriers to Threat Information Sharing Between Government and the Private Sector to ensure that IT Service Providers are able to share information with the government
- Modernize and Implement Stronger Cybersecurity Standards in the Federal Government to help move the Federal Government to secure cloud services and a zero-trust architecture, and mandates deployment of multifactor authentication and encryption within a specific time
- Improve Software Supply Chain Security to improve the security of software by establishing baseline security standards for development of software sold to the government
- It also creates a pilot program to create an “energy star” type of label so the government can quickly determine whether software was developed securely
- Establish a Cyber Safety Review Board to analyze what happened and make concrete recommendations for improving cybersecurity
- Create Standardized Playbook for Responding to Cybersecurity Vulnerabilities and Incidents to ensure all federal agencies meet a certain threshold and are prepared to take uniform steps to identify and mitigate a threat
- Improve Detection of Cybersecurity Incidents on Federal Government Networks to improve the ability to detect malicious cyber activity on federal networks by enabling a government-wide endpoint detection and response (EDR) system and improved information sharing
- Improve Investigative and Remediation Capabilities by creating cybersecurity event log requirements for federal departments and agencies

The main requirements of the Cybersecurity Enactment Act of 2014 were:

- NIST shall facilitate and support on an ongoing basis the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure (so this act basically established NIST and its role)
- Heads of the applicable federal agencies and departments shall develop and update every 4 years a Federal cybersecurity research and development strategic plan
- Director of the National Science Foundation shall support research that develops, evaluates, disseminates, and integrates new cybersecurity practices and concepts into the core curriculum of computer science programs and of other programs and develops new models for professional development of faculty in cybersecurity education, including secure coding development
- NIST shall, as necessary, develop and revise security automation standards, associated reference materials (including protocols), and checklists that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government
- OPM shall support competitions and challenges to identify, develop, and recruit talented individuals to perform duties relating to the security of information technology in Federal, State, local, and tribal government agencies, and the private sector
- NIST shall continue to coordinate a national cybersecurity awareness and education program
- Shall ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security
- Shall continue to develop and encourage the implementation of a comprehensive strategy for the use and adoption of cloud computing services by the Federal Government (Al noted that it was interesting that security of cloud computing was initiated this early in 2014, although apparently not much was done since it is still a big issue in 2023)
- Shall continue a program to support the development of voluntary and cost-effective technical standards, metrology, testbeds, and conformance criteria

This act set up NIST, NSF and the government activities to foster cybersecurity education and curriculums.

The Cybersecurity Enactment Act of 2015 built upon the Cybersecurity Enactment Act of 2014 with the requirements to:

- Authorize a government- wide intrusion detection and prevention system, operated by DHS, to apply the intrusion detection and prevention system to all information traveling to and from their information systems
- Require that agencies implement important cybersecurity best practices, such as encryption of sensitive data and multi-factor authentication for high-risk users (this was the key requirement of this act in Al's opinion)
- Ensure agencies proactively seek out adversaries that may have already established a presence in their networks through a requirement that the Office of Management and Budget (OMB) and DHS create an intrusion assessment plan
- Require the Director of OMB and the Secretary of Homeland Security to prioritize advanced security tools for network monitoring, including within the Continuous Diagnostics and Mitigation (CDM) program
- Require the Director of National Intelligence to identify information systems, which although unclassified, could reveal classified information if compromised
- Requires an assessment of the impact of the 2015 data breach at the Office of Personnel Management (OPM)
- Authorize the Secretary of DHS, in response to substantial threats, to issue directives to the heads of other agencies to take lawful action to protect their information systems and take direct action in response to imminent threats
- Includes reporting and oversight requirements to ensure effective implementation

Al then went through the cybersecurity roles of the three main government players – NIST, CISA and DHS

- NIST
    - Develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public (that's the role most of us know)
    - Some NIST cybersecurity assignments are defined by federal statutes, executive orders and policies. For example, the Office of Management and Budget (OMB) mandates that all federal agencies implement NIST's cybersecurity standards and guidance for non-national security systems (wasn't aware of this). Activities also are driven by the needs of U.S. industry and the broader public
    - Advances understanding and improves the management of privacy risks, some of which relate directly to cybersecurity
    - Priority areas to which NIST contributes – and plans to focus more on – include cryptography, education and workforce, emerging technologies, risk management, identity and access management, measurements, privacy, trustworthy networks and trustworthy platforms
- DHS (Department of Homeland Security)

  DHS has many departments under it like US Coast Guard, TSA and US Secret Service; each one has its specific role in cybersecurity that mostly deals with enforcement as shown in Slide 29.

  One that stands out is the Cyber Safety Review Board (CSRB) which is an independent public-private advisory body administered by DHS through CISA that brings together public and private sector cyber experts/leaders to review and draw lessons learned from the most significant cyber incidents
- CISA (Cybersecurity and Infrastructure Security Agency) (See https://www.cisa.gov/)
    - Is under DHS

- Works with partners to defend against today's threats and collaborates to build a more secure and resilient infrastructure for the future
- Leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure
- Main roles:
  - Are the Operational Lead for Federal Cybersecurity

    Coordinates the execution of our national cyber defense, leading asset response for significant cyber incidents and ensures that timely and actionable information is shared across federal and non-federal and private sector partners
  - We Are the National Coordinator for Critical Infrastructure Security and Resilience

  Work with partners across government and industry to defend against today's threats while securing the nation's critical infrastructure against threats that are just over the horizon

Al then began the second part of the special topic – a discussion of various cybersecurity frameworks. Al noted that the term "framework" is being used very loosely in this presentation, because some of the frameworks discussed are actually a set of security controls rather than an actual framework in the traditional sense.

Al found that surprisingly multiple frameworks exist that are developed by both US Government agencies and industry associations. The list of frameworks that Al was to discuss are:

- NIST Framework for Improving Critical Infrastructure Cybersecurity
- Center for Internet Security Critical Security Controls
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
- International Society of Automation ISA/IEC 62443
- International Telecommunications Union (ITU) National Cybersecurity / Critical Information Infrastructure Protection (CIIP)
- Internet of Things Security Foundation (IoTSF) Security Assurance Framework
- ISO/IEC 27001 / ISO/IEC 27002
- NIST SP 800-53R5

Note: Ira mentioned that there will be the US NIST Journey to Cybersecurity Framework 2.0 Workshop#2 at 9am-5:30pm on Wed 15 February 2023 - https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2.

- The NIST Framework for Improving Critical Infrastructure Cybersecurity was covered in detail at a previous IDS WG meeting but is outlined here.

  Version 1.1 was issued April 16, 2018. Its goal is to provide a common taxonomy and mechanism for organizations to (1) describe their current cybersecurity posture. (2) describe their target state for cybersecurity, (3) identify and prioritize opportunities for improvement within the context of a continuous and repeatable process, (4) assess progress toward the target state and (5) communicate among internal and external stakeholders about cybersecurity risk

  The NIST Cybersecurity Framework has three main components:

  - Framework Core - a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. It consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover. Each function identifies underlying key Categories and Subcategories which are discrete outcomes.
  - Framework Implementation Tiers ("Tiers") - Describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). This is similar

to the maturity levels in the Capability Maturity Model that assesses an organization's software process maturity.

- Framework Profile ("Profile"): represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. This is essentially a snapshot of the scores of the Framework core functions categories and subcategories for an organization at a single point in time.

The five Framework Core functions in more detail are:

Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. This is developing the infrastructure to implement cybersecurity functions

Protect – Develop and implement appropriate safeguards to ensure delivery of critical services. This is the actual implementation of the cybersecurity functions to try to prevent occurrences of cybersecurity incidents.

Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. This is the detection of actual cybersecurity incidents.

Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. This involves mitigation and other actions in response to cybersecurity incidents.

Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident, This includes things like backup plans recovery of systems to some type of operational state after a cybersecurity incident.

Ira noted that NIST also has the NIST Risk Management Framework (RMF) at https://csrc.nist.gov/projects/risk-management/about-rmf.

NIST also developed sector-specific cryptographic frameworks for critical sectors. The critical sectors that specific frameworks were created for were:

- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Federal
- Healthcare & Public Health
- Nuclear Framework Guidance
- Transportation Systems
- Water & Wastewater Systems

- Center for Internet Security (CIS) Critical Security Controls

  This framework was issued in May 2021 and had, as its purpose, to:
  - Share insights into attacks and attackers, identify root causes, and translate that into classes of defensive action
  - Create and share tools, working aids, and stories of adoption and problem-solving

- Map the CIS Controls to regulatory and compliance frameworks to ensure alignment and bring collective priority and focus to them Identify common problems and barriers (like initial assessment and implementation roadmaps), and solve them as a community
- Reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals), with every role (threat responders and analysts, technologists, information technology (IT) operators and defenders, vulnerability-finders, tool makers, solution providers, users, policy-makers, auditors, etc.), and across many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT, etc.)

The maim point here was the sharing of knowledge across many groups and roles to get the varied perspectives on what security control are most needed.

Slides 38-40 list the various categories of security controls included in the CIS Critical Security Controls. Some of the more interesting ones are:

- **Inventory and Control of Enterprise Assets:** Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments to support identifying unauthorized and unmanaged assets to remove or remediate - this applies to all the chips that go into your car, refrigerator, medical equipment like pacemakers, etc.
- **Inventory and Control of Software Assets:** Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution – again a critical control
- **Data Protection:** Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data – data protection is a foundation of security
- **Secure Configuration of Enterprise Assets and Software:** Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications) – it is a critical customer ask that the security configuration of enterprise assets be set up, documented, and maintained
- **Account Management**: Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software – managing user accounts and access control below are two critical admin functions to ensuring only authorized users perform intended functions
- **Access Control Management:** Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software
- **Continuous Vulnerability Management:** Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, to remediate, and minimize, the window of opportunity for attackers and monitor public and private industry sources for new threat and vulnerability information. Ira noted here that CISA maintains Weekly Vulnerability Summaries at https://www.cisa.gov/uscert/ncas/bulletins.
- **Audit Log Management:** Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack – reinforces the importance of maintaining and checking audit logs
- **Data Recovery**: Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state – goes along with the Recovery Function in the NIST Cybersecurity Framework
- **Application Software Security**: Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before

they can impact the enterprise – interesting to see a control on the in-house development of software apps

- **Penetration Testing:** Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker – this one was the most interesting that the CIS controls require penetration testing to try to force the system to exploit known vulnerabilities; Al hadn't seen this in any other such frameworks previously.

- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

  The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) is a cybersecurity control framework for cloud computing. Al tried but was unable to obtain a copy of this matrix; all he was able to obtain was the following general facts:

  - Composed of 197 control objectives that are structured in 17 domains covering all key aspects of cloud technology
  - Used as a tool for the systematic assessment of a cloud implementation, and provides guidance on which security controls should be implemented by which actor within the cloud supply chain
  - Is aligned to the CSA Security Guidance for Cloud Computing, and is considered a de-facto standard for cloud security assurance and compliance
  - Includes the following:

    CCM v4 Controls – the actual CCM

    - Mappings
    - CAIQ v4
    - Implementation Guidelines
    - Auditing Guidelines
    - CCM Metrics

  Note that some actual links are provided here that may provide the reader with some better insights into the CSA CCM.

- International Society of Automation ISA/IEC 62443

  ISA/IEC 62443 is an international series of standards that address cybersecurity for operational technology in automation and control systems. The goals of these standards are to:

  - improve the safety, availability, integrity and confidentiality of components or systems used for industrial automation and control, and
  - Provide criteria for procuring and implementing secure industrial automation and control systems

  These standards are directed towards those responsible for designing, implementing, or managing industrial automation and control systems, and apply to users, system integrators, security practitioners, and control systems manufacturers and vendors. The ISA/IEC 62443 standards build on the ISO/IEC 27000 series of standards.

  Slides 43 and 44 list the specific standards that are part of the ISA/IEC 62443 set. However, they fall into the following TBD categories:

  - **General** – This group includes elements that address topics that are common to the entire series
  - **Policies and Procedures** – Elements in this group focus on the policies and procedures associated with Industrial Automation and Control Systems (IACS) security
  - **System Requirements** – Elements in the third group address requirements at the system level

- **Component Requirements** – Fourth and final group includes elements that provide information about the more specific and detailed requirements associated with the development of IACS products

- International Telecommunications Union (ITU) National Cybersecurity / Critical Information Infrastructure Protection (CIIP)

  Critical Information Infrastructure Protection (CIIP) is a vital component of national security policy. CIIP includes multiple aspects, ranging from reducing vulnerabilities and fighting computer crime to defense against cyber-terrorism.

  The ITU CIIP Framework was developed in August 2007 to help countries to determine their response to the challenges of CIIP. The framework itself draws on different existing CIIP models, in particular, the Swiss CIIP model, to suggest a functional model for a CIIP unit that can promote collaboration between existing stakeholders to protect the state's critical infrastructure and services

  The framework is based on the four pillars of CIIP:

  - **Prevention and Early Warning** - Ensure that companies operating critical infrastructures are prepared to cope with incidents through activities that raise the general preparedness of companies and ensure that critical infrastructures "are less vulnerable to disruptions".
  - **Detection** – Ensure that new threats be discovered as quickly as possible. Also, ensure non-technical analyses of the general risk situation are performed and technical as well as non-technical information are shared with international partners
  - **Reaction** - Includes the identification and correction of the causes of a disruption. Also, provide advice and guidance on how to tackle an incident, rather than offering complete solutions when appropriate
  - **Crisis Management** - Minimize the effects of any disruptions on society and the state

- Internet of Things Security Foundation (IoTSF) Security Assurance Framework

  The IoTSF Security Assurance Framework Release 3.0 was released in November 2021. Rather than providing a set of controls. This framework is a structured process of questioning and evidence gathering to ensure suitable security mechanisms and practices are implemented.

  This framework is intended to help all companies make high-quality, informed security choices by guiding them through a comprehensive requirement checklist and evidence gathering process; the evidence gathered during the process can be used to declare conformance with best practice to customers and other stakeholders.

  The results of this process can be used internally in an organization as a pre-compliance tool to self-assess or self-certify against, or by a third-party auditor. They can also be used 'in part', as a procurement mechanism to help specify security requirements of a supplier contract.

  The IoTSF Security Assurance Framework's stakeholders are:

  - Managers in organizations that provide IoT products, technology and or services
  - Developers and Engineers, Logistics and Manufacturing Staff, it provides detailed requirements to use in their daily work and in project reviews to validate the use of best practice by different functions (e.g., hardware and software development, logistics etc.
  - Supply Chain Managers, the structure can be used to guide the auditing of security practices

  and the scope of the Framework is:

  - Business processes
  - The "Things" in IoT, i.e., network connected products and/or devices
  - Aggregation points such as gateways and hubs that form part of the connectivity
  - Networking including wired, and radio connections, cloud and server elements

The Framework's process contains three steps:

- **Risk Assessment** - Conduct Risk Analysis of product in target environment (i.e., actually performing the Risk Assessment)
- **Assurance Class** - Determine Assurance Class applicable to the product
- **Using the Assurance Questionnaire** - Respond to each question in the framework document (this is what distinguishes this from other frameworks)

Similar to the NIST Cybersecurity Framework, the IoTSF Security Assurance Framework created questionnaires for the following different categories:

- Business Security Processes, Policies and Responsibilities
- Device Hardware & Physical Security
- Device Software
- Device Operating System
- Device Wired and Wireless Interfaces
- Authentication and Authorization
- Encryption and Key Management for Hardware
- Web User Interface
- Mobile Application
- Privacy
- Cloud and Network Elements
- Secure Supply Chain and Production
- Configuration
- Device Ownership Transfer

Al noted that several of the categories like the Encryption and Key Management and Authentication and Authorization are categories you would expect to find in such a framework.

- ISO/IEC 27001 / ISO/IEC 27002
  - ISO 27001 Information technology — Security techniques — Information security management systems

    ISO 27001 is an international standard for the implementation of an enterprise-wide Information Security Management System (ISMS). The current version per Ira is in 2022.

    ISO 27001 covers all types of organizations (e.g., commercial enterprises, government agencies, non-profit organizations). It specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks that are customized to the needs of individual organizations or parts thereof. ISO/IEC 27001 security controls are designed to protect information assets and give confidence to interested parties.

    The ISO 27001 standard is required by:

    - Organizations carrying sensitive information, regardless of their size, be it public or private, IT or non-IT
    - Organizations expanding their business and seeking new clients
    - Contractors that need to be ISO 27001 compliant to score projects

    ISO 27001 provides security controls for the following domains:

- Security Policy
- Organization of Information Security
- Asset Management
- Human Resourced Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management
- Compliance

- ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security management

  ISO 27002 is a companion to ISO 27001. It establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization and provides general guidance on the commonly accepted goals of information security management. Like ISO 27001, the current version per Ira is in 2022.

  Control objectives and controls in ISO 27002 are intended to be implemented to meet the requirements identified by a risk assessment. The main clauses are the same as the main categories in ISO/IEC 27001 listed above; each clause has one or more main security categories that provide the following additional information above what ISO 27001 provides:

  - Control objective
  - Controls that can be applied to achieve the control objective.
  - A specific control statement to satisfy the control objective.
  - Implementation guidance
  - Further information that may need to be considered

- NIST SP 800-53R5

  NIST SP 800-53R5 (dated Sep 2020) provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks. It is considered the “gold standard” of the list of security controls for information systems used in the US by industry and the government.

  NIST SP 800-53R5 lists a large set of security controls for the following control families:

• Access Control	• Authorization and Monitoring	• Physical and Environmental Protection	• Program Management
• Audit and Accountability	• Identification and Authentication	• Planning	• PII Processing and Transparency
• Awareness and Training	• Incident Response	• Risk Assessment	• Supply Chain Risk Management

• Configuration Management	• Maintenance	• System and Services Acquisition	• System and Communications Protection
• Contingency Planning	• Media Protection	• System and Information Integrity	
• Assessment	• Personnel Security		

6. Since Ira had already indicated at the Plenary session that nothing had been done on the HCD Security Guidelines, it was decided that this topic could be skipped for this session..
7. For the final topic, Ira presented his Liaison report on current standards developments for the Trusted Computing Group (TCG) and Internet Engineering Task Force (IETF). The key points from Ira's Liaison Report were:
    - Regarding TCG standards activities, some key items Ira mentioned were:
        - Next TCG Members F2F Meetings will be 21-23 February 2023 in Vancouver BC and the 3rd or 4th week of June 2023 in Munich Germany. Both will be hybrid meetings and Ira will call into both.
        - Regarding **Trusted Mobility Solutions (TMS)**, it is developing several new protocols that are not listed on Slide 56..
        - For **Mobile Platform (MPWG)**:
            - ***TCG Mobile Reference Architecture v2*** will be in public review in March 2023.
            - ***TCG TPM 2.0 Mobile Common Profile*** has been delayed and deferred.
        - For **Recent Specs**
            - ***TCG Storage Interface Interactions Spec (SIIS)*** went into public review December 2022.
            - ***TCG DICE Endorsement Architecture for Devices*** was published November 2022.
            - ***TCG Component Class Registry*** and ***TCG Storage Component Class Registry*** have both been posted since November.
    - Regarding IETF standards activities, some key items Ira stressed were:
        - **IETF 116 F2F** will be in Yokohama, Japan on 27-31 March 2023 and **IETF 117 F2F** will be in San Francisco, CA) on 24-28 July 2023. Both will be Hybrid meetings and Ira to call in.
        - For TLS:
            - Are no new RFCs
            - **IETF IANA Registry Updates for TLS/DTLS** will soon be in formal review
            - **IETF Identity Module for TLS Version 1.3** had a recent draft in January 2023
            - **IETF Flags Extension for TLS 1.3** – recent draft was adopted by the WG
            - **IETF Compact TLS 1.3** will soon be in IETF Last Call
            - **IETF NULL Encryption & Key Exchange w/o Forward Secrecy Discouraged** will soon be WG adopted

- **IETF Compact ECDHE and ECDSA Encodings for TLS 1.3** is an important new spec
- **IETF Suppressing CA Certificates in TLS 1.3** involves optimization
- **IETF Deprecating Obsolete Key Exchange Methods in TLS** was adopted by the WG

- For **Security Automation and Continuous Monitoring (SACM), IETF Concise Software Identifiers** is finally moving along.
- **Concise Binary Object Representation (CBOR**
  - No new RFCs
  - **IETF CBOR Tags for Time, Duration, and Period** will create its RFC by 3Q 2023
  - **IETF App-Oriented Literals in CBOR Ext Diag Notation** is an important Spec for debugging purposes
  - **IETF CDDL 2.0** will soon be WG adopted
  - **IETF Notable CBOR Tags** will soon get registered
- Regarding **Remote ATtestation ProcedureS (RATS)**:
  - **IETF CBOR Tag for Unprotected CWT Claims Sets** is in IETF Last Call
  - **IETF RATS Architecture** as recently published as RFC 9334 in January 2023
  - **IETF Concise TA Stores (CoTS)** has been WG adopted
  - **IETF EAT-based Key Attestation Token** and **IETF RATS Conceptual Messages Wrapper** are both specs of interest
- Finally, for the **IRTF Crypto Forum Research Group (CFRG):**
  - **IRTF Argon2 password hash and proof-of-work** was published as RFC 9106 in September 2021sent to Internet Research review
  - **IRTF RSA Blind Signatures** went to the IRTF Chair and soon will go to IETF Last Call
  - **IRTF AEGIS family of authenticated encryption algorithms** has been WG adopted
  - **IRTF Two-Round Threshold Schnorr Sigs with FROST** will soon be going to IETF Last Call
  - **IRTF CPace, a balanced composable PAKE** has been CFRG adopted
  - **IRTF Properties of AEAD algorithms** involves usage limits on AEAD
  - **IRTF Deterministic Nonce-less HPKE** has been WG adopted
  - **IRTF Ristretto255 and Decaf448 Groups** involves extensions
  - **IRTF Combiner for Hybrid Key Encapsulation Mechanisms** was just adopted

At the end of the Liaison Report Ira mentioned that to implement CNSA 2.0 there will be a need to transition to hybrid algorithms. Ira also felt that eventually there will be a need for a CNSA 3.0 because the hash-based algorithms chosen for CNSA 2.0 are impractical for most apps in use today.

8. **Wrap Up**

- Next IDS Working Group Meeting will be on February 23, 2023. Main topics of the meeting will be the latest status of the HCD iTC and HCD cPP/SD and a Special Topic that is yet to be determined. If Ira attends the meeting we will discuss how we can help get development of the HCD Security Guidelines moving again. .

- Next IDS Face-to-Face Meeting will be during the May 2023 PWG Virtual Face-to-Face Meeting May 16-18, 2023 (likely on May 18, 2023).

Actions: There were no actions resulting from this meeting.

The meeting was adjourned at 12:00 N ET on February 9, 2023.