IDS WG Meeting Minutes
February 23, 2023

This IDS WG Meeting was started at approximately 3:00 pm ET on February 23, 2023.

Attendees

Jerry Colunga	HP
Graydon Dodson	Lexmark
Smith Kennedy	HP
Alan Sukert	
Bill Wagner	TIC

Agenda Items

1. The topics to be covered during this meeting were:
   - Latest status on the HCD iTC
   - Special topics on NIST SP 800-171R2
   - Round Table
2. Meeting began by stating the PWG Anti-Trust Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-antitrust-policy.pdf and the PWG Intellectual Property Policy which can be found at https://www.pwg.org/chair/membership_docs/pwg-ip-policy.pdf.
3. Al gave a quick status of the HCD iTC.
   - The good news is that since the IDS Session on February 9th at the PWG February Face-to-Face Meetings, two important things happened:
     - The Canadian Scheme submitted a positive Endorsement supporting HCD cPP v1.0 on February 7th
     - JISEC submitted a Position Statement that supports HCD cPP v1.0 and HCD SD v1.0 and indicates it will accept applications for certifications against the HCD cPP.

     NIAP and ITSCC are still reviewing the documents.
   - Ira McDonald indicated at the meeting that the ND iTC is still addressing issues against ND cPP v3.0 but expects to publish this version by the end of March 2023.
   - Al then shared the infrastructure he has set up for the HCD Interpretation Team (HIT). It consists of two main items:
     - A separate HIT repository so that the HIT can create updates to HCD cPP v1.0 and HCD SD 1.0 without affecting the main repositories that will be working on v1.1. Right now, there are Working and Master baselines, but more will be created as needed.
     - Working with Brain Wood, based on what the DSC IT is doing Al created an Interpretation Team Project that can be used to track RfI Issues as they go through the phases of the HIT process as documented in the HIT procedures. This project is essentially a spreadsheet that can be used to move an RfI from 'Todo' → 'Awaiting Priority' → 'Awaiting Review' → 'In Progress' → 'Completed' and provide a visual look at the status of each RfI

       Al plans to test this process with the full HIT using an issue against HCD cPP v1.0 that Tom Benkart sent to Al.
4. Al presented this week's special topics on NIST Special Publication 800-171 Revision 2 (NIST SP 800-171R2), Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. The slides Al used can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/NIST SP 800-171R2.pdf.

   The main items covered in the presentation were:

- NIST SP 800-171R2 was published in February 2020 and can be found at https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final. The goal of this document is to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI (Confidential Unclassified Information):
  - When the CUI is resident in a non-federal system and organization
  - When the non-federal organization is *not* collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency and
  - Where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry

  Al noted that based on the above the intent of NIST SP 800-171 is to apply to large "enterprise-like" organizations rather that small organizations like a doctor's office (see more on that later).

  NIST SP 800-171R2 applies to components of nonfederal systems that **process, store, or transmit CUI, or that provide security protection for such components**.

- The target audience for NIST SP 800-171 is persons with:
  - System development life cycle responsibilities (e.g., program managers, mission/business owners, information owners/stewards, system designers and developers, etc.)
  - Acquisition or procurement responsibilities (e.g., contracting officers)
  - System, security, or risk management and oversight responsibilities (e.g., authorizing officials, chief information officers, chief information security officers, etc.) and
  - Security assessment and monitoring responsibilities (e.g., auditors, system evaluators, assessors, independent verifiers/validators, etc.)

- Some key definitions needed to understand NIST SP 800-171:
  - **Controlled Unclassified Information:** Information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, *Classified National Security Information*, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended

    The best example of CUI is your medical information that must be protected because of HIPAA. Other examples of CUI are social security numbers, financial information due to the Graham-Leach-Bliley law, legal information. PII (Personal Identifiable Information) is just a subset of the totality of CUI. Essentially CUI is any unclassified information that must be protected due to a federal or state law.
  - **Availability**: Ensuring timely and reliable access to and use of information
  - **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
  - **Sanitization**: Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means
  - Also, Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs
  - **Hardware:** The material physical components of a system
  - **Integrity**: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
  - **Security**: A condition that results from the establishment and maintenance of protective measures that enable an organization to perform its mission or critical functions despite risks posed by threats to its use of systems

- **Security Control**: The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information
- **Security Functions**: The hardware, software, or firmware of the system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based

Al pointed out that the CIA definitions are not the standard definitions for confidentiality, integrity and availability. But was most interesting was that NIST SP 800-171 had definitions for firmware and hardware, but no definition for software.

- At this point Al stopped the discussion of NIST SP 800-171 and began a discission of a related topic – a law passed by the State of California in 2018 related to NIST SP 800-171 euphemistically called the "California Password Law", or official California SB-327.

  The "California Password Law" dealt with the "Security of Connected Devices". A couple of key definitions to understand the provisions of this law:

  - Connected Device: Any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address
  - Manufacturer: The person who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California
  - Security feature: A feature of a device designed to provide security for that device
  - Unauthorized access, destruction, use, modification, or disclosure: Access, destruction, use, modification, or disclosure that is not authorized by the consumer

  The key requirements of the "California Password Law" are as follows:

  - A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:
    - Appropriate to the nature and function of the device
    - Appropriate to the information it may collect, contain, or transmit.
    - Designed to protect the device and any information contained therein from unauthorized Subject to all of the requirements of subdivision
  - If a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:
    - **The preprogrammed password is unique to each device manufactured**
    - **The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time**

  What the two bolded requirements mean in effect are that every connected device manufactured and sold in California, and that would include HCDs, that performs network authentication must have (1) a unique preprogrammed default admin password and (2) a security feature that requires a user they first time that user logs into the device (and that includes the admin) to generate a unique password.

  Later in the presentation Al showed how this relates to NIST SP 800-171.

- Continuing the discussion of NIST SP 800-171, NIST SP 800-171 documents the 14 Security Requirements Families shown below:

Family	Family

Access Control	Media Protection
Awareness & Training	Personnel Security
Audit & Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification & Authentication	Security Assessment
Incident Response	System & Communications Protection
Maintenance	System & Information Integrity

Each Security Requirements family is defined by Basic Requirements, which are at a very high level; Derived Requirements, which are really more like guidelines than requirements; and a more detailed discussion of the basic requirements.

Slides 10-25 in the presentation list all of the Basic and Derived Requirements for each of the 14 Security Requirements Families. Below are the Basic and some of the key Derived Requirements Al pointed out for each family:

- **Access Control**

  Basic Requirements

  - Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems)
  - Limit system access to the types of transactions and functions that authorized users are permitted to execute

  Derived Requirements

  - Control the flow of CUI in accordance with approved authorizations
  - Separate the duties of individuals to reduce the risk of malevolent activity without collusion
  - Employ the principle of least privilege, including for specific security functions and privileged accounts
  - Use non-privileged accounts or roles when accessing non-security functions
  - Limit unsuccessful logon attempts
  - Monitor and control remote access sessions
  - Employ cryptographic mechanisms to protect the confidentiality of remote access sessions
  - Protect wireless access using authentication and encryption
  - Encrypt CUI on mobile devices and mobile computing platforms

  Al noted that this family had by far the largest number of Derived Requirements.

- **Awareness and Training**

  Basic Requirements

  - Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems
  - Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities

Derived Requirement

- Provide security awareness training on recognizing and reporting potential indicators of insider threat

Al noted this is what would be expected for this family, especially the security awareness training.

- **Audit and Accountability**

  Basic Requirements

  - Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity
  - Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions

  Derived Requirement

  - Review and update logged events
  - Alert in the event of an audit logging process failure
  - Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity
  - Provide audit record reduction and report generation to support on-demand analysis and reporting
  - Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records
  - Protect audit information and audit logging tools from unauthorized access, modification, and deletion
  - Limit management of audit logging functionality to a subset of privileged users

  Al noted this many of the Derived Requirements for this family (like ”Protect audit information and audit logging tools from unauthorized access, modification, and deletion” are SFRs in the HCD cPP).

- **Configuration Management**

  Basic Requirements

  - Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles
  - Establish and enforce security configuration settings for information technology products employed in organizational systems

  Derived Requirement

  - Track, review, approve or disapprove, and log changes to organizational systems
  - Analyze the security impact of changes prior to implementation
  - Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems
  - Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities
  - Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services

- Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
- Control and monitor user-installed software

Al noted this is not an area of expertise for him, so he just listed the Derived Requirements. He especially didn't understand what deny-by-exception and deny-all, permit-by-exception were.

- **Identification and Authentication**

  Basic Requirements

  - Identify system users, processes acting on behalf of users, and devices
  - Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems

  Derived Requirement

  - Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts
  - Employ replay-resistant authentication mechanisms for network access to privileged and nonprivileged accounts
  - Prevent reuse of identifiers for a defined period
  - Disable identifiers after a defined period of inactivity
  - **Enforce a minimum password complexity and change of characters when new passwords are created**
  - **Prohibit password reuse for a specified number of generations**
  - **Allow temporary password use for system logons with an immediate change to a permanent password**
  - **Store and transmit only cryptographically-protected passwords**
  - Obscure feedback of authentication information

  This family is where you can really see how high-level the Basic Requirements are.

  Al focused on the four bolded password-related Derived Requirements - note that "**Allow temporary password use for system logons with an immediate change to a permanent password**" is very similar to the second of the two password requirements in the "California Password Law"; **Enforce a minimum password complexity and change of characters when new passwords are created** is similar to some potential requirements to put 30, 60 or 90 day limits on user passwords on HCDs; **Prohibit password reuse for a specified number of generations** is similar to what many of us experience when we try to change our password on one of our accounts and are told we cannot use any previous passwords; and finally **Store and transmit only cryptographically-protected passwords** is just sound guidance for any password.

- **Incident Response**

  Basic Requirements

  - Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities
  - Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization

  Derived Requirement

  - Test the organizational incident response capability

This is as should be expected.

- **Maintenance**

  Basic Requirements

  - Perform maintenance on organizational systems
  - Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance

  Derived Requirement

  - Ensure equipment removed for off-site maintenance is sanitized of any CUI
  - Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems
  - Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete
  - Supervise the maintenance activities of maintenance personnel without required access authorization

  Again, this is as should be expected.

- **Media Protection**

  Basic Requirements

  - Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital
  - Limit access to CUI on system media to authorized users
  - Sanitize or destroy system media containing CUI before disposal or release for reuse
    - Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is released for reuse or disposal

  Derived Requirement

  - Mark media with necessary CUI markings and distribution limitations
  - Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas
  - Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards
  - Control the use of removable media on system components
  - Prohibit the use of portable storage devices when such devices have no identifiable owner
  - Protect the confidentiality of backup CUI at storage locations

  Al noted that sanitization in the content of NIST SP 800-171 included cryptographic erase. He also noted from his time at Xerox the importance of protecting backups. Overall, protection of media is more important than one would think.

- **Personnel Security**

  Basic Requirements

  - Screen individuals prior to authorizing access to organizational systems containing CUI
  - Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers

Derived Requirement - None

Not much needed to be said for this family.

- **Physical Protection**

  Basic Requirements

  - Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals
  - Protect and monitor the physical facility and support infrastructure for organizational systems

  Derived Requirement

  - Escort visitors and monitor visitor activity
  - Maintain audit logs of physical access
  - Control and manage physical access devices
  - Enforce safeguarding measures for CUI at alternate work sites

  This is one of our assumptions in the HCD cPP.

- **Risk Assessment**

  Basic Requirements

  - Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI

  Derived Requirement

  - Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified
  - Remediate vulnerabilities in accordance with risk assessments

  Another case of very high-level Basic Requirements, given NIST has an entire framework around risk management. The Derived Requirements were also limited in that they only focused on vulnerability management; risk assessment is more than just vulnerability scanning.

- **Security Assessment**

  Basic Requirements

  - Periodically assess the security controls in organizational systems to determine if the controls are effective in their application
  - Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems
  - Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls
  - Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems

  Derived Requirement - None

  This shows the “closed loop” aspect by requiring that the security controls implemented be assessed to determine if they are effective, and if not adjusted accordingly. This is something that is seen regularly in the EU laws also.

- **System and Communications Protection**

  Basic Requirements

  - Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems
  - Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems

  Derived Requirement

  - Prevent unauthorized and unintended information transfer via shared system resources
  - Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks
  - Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception)
  - Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling)
  - Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards
  - Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity
  - Establish and manage cryptographic keys for cryptography employed in organizational systems
  - Employ FIPS-validated cryptography when used to protect the confidentiality of CUI
  - Control and monitor the use of mobile code
  - Protect the authenticity of communications sessions
  - Protect the confidentiality of CUI at rest

  Still another case of very high-level Basic Requirements. In many cases the Derived Requirements (e.g., Protect the confidentiality of CUI at rest) would be better Basic Requirements than the ones they currently have. Also, you'd expect NIST would require FIPS-validated cryptography here.

- **System and Information Integrity**

  Basic Requirements

  - Identify, report, and correct system flaws in a timely manner
  - Provide protection from malicious code at designated locations within organizational systems
  - Monitor system security alerts and advisories and take action in response

  Derived Requirement

  - Update malicious code protection mechanisms when new releases are available
  - Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed
  - Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks
  - Identify unauthorized use of organizational systems

This is effectively Flaw Remediation. However, Flaw Remediation should be more that scans and malware protection; there are no Derived Requirements associated with the Basic Requirement to “Identify, report, and correct system flaws in a timely manner”.

- There is tailoring guidance included in NIST SP 800-171 for each of the 14 Security Requirements Families. The criteria for tailoring are based on three factors:
  - The control or control enhancement is uniquely federal (i.e., primarily the responsibility of the federal government)
  - The control or control enhancement is not directly related to protecting the confidentiality of CUI
  - The control or control enhancement is expected to be routinely satisfied by non-federal organizations without specification

  The problem is that since NIST SP 800-171 is design for larger organizations that do business with the government, this tailoring is not meaningful for smaller organizations that have to protect CUI such as medical, legal or financial information and which don’t do business directly with the government. Al felt what is needed is either tailoring guidance or a version of NIST SP 800-171 that is focused on smaller organizations that have protect CUI.

- The final discussion was on when NIST SP 800-171 is required. Al indicated that based on the available information, any organization that processes, stores or transmits CUI for the DoD, GSA or NASA, and other federal or state agencies, including subcontractors must comply with NIST SP 800-171. It is recommended for other organizations that do not do business with federal or state agencies

  Bill asked about enforcement of NIST SP 800-171. Al indicated that when NIST SP 800-171 was first documented back in 2018 and set to go in effect in 2020, NIST indicated there would be harsh penalties if it was not complied with. However, since NIST SP 800-171 was scheduled to go into effect just as Covid hit, it is not clear what enforcement if any has been put in place since then. There are a lot of consulting firms making money off of NIST SP 800-171 compliance, but there is nothing about compliance on the NIST SP 800-171 web site so it might not even be on NIST’s radar at this time.

5. Round Table:
   - Al mentioned that the CCUF Spring 2023 Workshop will be a virtual workshop held on March 8th and 9th.
6. **Actions:** None

Next Steps

- The next IDS WG Meeting will be March 23, 2023 at 3:00P ET / 12:00N PT because Al will be on vacation on March 9th, which would have been the date for our next regularly scheduled meeting. Main topics will be the latest tatus of the HCD iTC and a TBD special topic..