IDS WG Meeting Minutes
August 24, 2023

This IDS WG Meeting was started at approximately 3:00 pm ET on July 27, 2023.

Attendees

Jerry Colunga	HP
Graydon Dobson	Lexmark
Jeremy Leber	Lexmark
Alan Sukert	
Mike Trent	Xerox
Brian Volkoff	Ricoh
Bill Wagner	TIC

Agenda Items

1. The topics to be covered during this meeting were:
    - Latest updates on the HCD iTC and the HCD Interpretation Team (HIT)
    - Special Topic on some surprising additional US Cybersecurity Laws
    - Special Topic on the proposed update to NIST SP 800-171r3 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
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 began discussing the results of the August 21st HCD iTC Meeting.
    - It looks like the Korean Scheme will probably provide an Endorsement Statement for HCD cPP/SD v1.0 at the Fall 2023 CCDB Meetings the end of October.
    - Kwangwoo Lee indicated that it is likely that the HCD iTC will get comments against HCD cPP v1.0 from some of the Schemes other than NIAP and Canada. Jerry asked how many comments we might expect; Al indicated his sense was not many but he had no sense of whether the comment would be mostly editorial type comments like we have received from NIAP and the Canadian Scheme so far or more technical comments. Al said he would check with Kwangwoo and Anantha Kandia what types of comments the ND iTC received for the ND cPP.
    - As Al had mentioned at the IDS Session at the recent PWG August Virtual Face-to-Face Meetings on Aug 10th, the CCDB had issued a draft Specification of Functional Requirements for Cryptography that Al had reviewed and compared against the crypto SFRs in HCD cPP v1.0. He and others on the HCD iTC had sent comments against this draft specification to the CCDB. The HCD iTC is waiting to see what is in the final version of this spec and what the directions for implementing this spec will be.
    - Kwangwoo indicated that NIAP had 53 technical comments against ND cPP v3,0, mostly against the TLS 3.0 implementation in the document. The HCD iTC will wait until the ND TLS subgroup resolves these comments before it will integrate the ND iTC TLS 3.0 solution into the HCD cPP/SD.
    - As Al indicated in his IDS Session at the PWG August Virtual Face-to-Face, the HCD iTC will wait until NIAP issues its plan for CNSA 2.0 implementation before having discussions with NIAP on including CNSA 2.0 in the HCD cPP/SD..
    - The Fall 2023 CCUF Workshop will ne 26-30 Oct in Wash DC. There will be an HCD iTC/HIT Meeting at the Workshop; currently it is scheduled for Friday Oct 27th but Kwangwoo is trying to move it to Monday Oct 30th.

- The 2023 International Common Criteria Conference will be 31 Oct – 2 Nov in Wash DC,

4. Al next gave an update on the HIT.

   - There are currently ten open HIT issues, including a new issue HCD-IT #11. Issue HCD-IT #11 is titled "**In FCS_CKM.4 Cryptographic key destruction, clarification needed whether encrypted keys stored in non-volatile memory are within the scope of key destruction**".

     The issue here is that for Section 5.3.5 **FCS_CKM.4 Cryptographic key destruction** in the HCD cPP, it is not clear that encrypted keys stored in non-volatile memory is within the scope of key destruction. The suggested change is to describe in an Application Note whether encrypted keys stored in non-volatile memory are within the scope of key destruction or not.

     The key to the issue is the word "encrypted" in the Issue statement. This Issue is also linked to Section 5.3.4, SFR **FCS_CKM_EXT.4 Extended: Cryptographic Key Material Destruction** and SFR 5.3.4.1 which states "**FCS_CKM_EXT.4.1** The TSF shall destroy all plaintext secret and private cryptographic keys and cryptographic critical security parameters when no longer needed." SFRs **FCS_CKM_EXT.4** and **FCS_CKM.4** were taken from the ND cPP v2.2e originally, but the original idea for **FCS_CKM.4** was that it applies to all keys, including encrypted keys, and not just plaintext keys. However, since **FCS_CKM_EXT.4** only applies to "plaintext secret and private cryptographic keys and cryptographic critical security parameters", someone looking at the HCD cPP could imply that **FCS_CKM.4** only applies to plaintext keys also.

     On the other hand, although **FCS_CKM.4** does not explicitly state that it applies to encrypted keys it could be interpreted to apply to non-volatile memory and to encrypted keys. There was even a suggestion of defining via an Application Note that a "cryptographic key" is.

     Therefore, the central question of this issue – should we be destroying all keys or just plaintext keys. The issue has been assigned and is being worked on.

   - As for the status of the other open issues:

     - Issue #1: Are working on a proposal to CFB mode support to the CCDB WG crypto catalog and provide it to Kwangwoo. Kwangwoo forward the proposal to a CCDB member.
     - Issue #2: Ohya-san and Al volunteered to review the changes to the SD. Jerry had a process question about where the push the fix; Al explained that the way the HIR Procedures are currently written you create the file with the version of the cPP or SD , as applicable, containing the fix in the Working baseline and you push the file with the fix into the Interpretation baseline.
     - Issues #4-7: Still being worked on by Brian.
     - Issue #8. Because the key person for this issue was not in attendance at the last HIT Meeting on 8/14, issue was deferred to the next HIT meeting on 8/28.
     - Issue #9: Awaiting resolution of Issue #2 so Jerry can work on this issue.
     - Issue #10: Tom Benkart has described his approach to address this issue; If Brian agrees with Tom's proposed approach, we can move forward.

   At the 8/21 HCD iTC Meeting Kwangwoo indicated that he needed the HIT to do two things at the next HIT Meeting regarding the 10 open issues:

   - Determine which of the10 issues are "low hanging fruit: and close them as quickly as possible
   - For the remaining issues prioritize them and work close them in the priority order.

5. Al then presented his special topic for the day, which is a look at some surprising additional US Cybersecurity Laws. The slides for this presentation can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/US Cybersecurity Legislation Part 2.pdf.

   a. Federal Trade Commission

      This topic all started because Al did a Google search on the term "cybersecurity laws" and this is exactly what Google came up with:

The primary law governing cybersecurity in the United States is the Federal Trade Commission Act (FTCA). This law prohibits deceptive acts and practices in business, including those related to data security

Now the Federal Trade Commission Act was signed into law by President Herbert Hoover in 1914, some 80+ years before anyone knew want cybersecurity was. So, the question is "What does the Federal Trade Commission Act have to do with cybersecurity?" Turns out it is more than you think.

The key provision of the Federal Trade Commission Act was to establish the Federal Trade Commission (FTC).The Federal Trade Commission Act empowered the FTC to:

- Prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce;
- Seek monetary redress and other relief for conduct injurious to consumers;
- Prescribe rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices;
- Gather and compile information and conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and
- Make reports and legislative recommendations to Congress and the public. A number of other statutes listed here are enforced under the FTC Act

The roles of the FTC are to:

- Enforce a variety of antitrust and consumer protection laws affecting virtually every area of commerce, with some exceptions concerning banks, insurance companies, non-profits, transportation and communications common carriers, air carriers, and some other entities The agency leverages its resources and targets its enforcement efforts at practices that cause the greatest harm to consumers.
- Investigate and prevent unfair methods of competition, and unfair or deceptive acts or practices affecting commerce
- Seek relief for consumers, including injunctions and restitution, and in some instances to seek civil penalties from wrongdoers
- Implement trade regulation rules defining with specificity acts or practices that are unfair or deceptive
- Publish reports and make legislative recommendations to Congress about issues affecting the economy
- Enforce various antitrust laws under Section 5(a) of the FTC Act as well as the Clayton Act. The FTC monitors all its orders to ensure compliance
- The FTC conducts regular reviews of all its rules and guides on a rotating basis to make sure they are up-to-date, effective, and not overly burdensome

The "antitrust and consumer protection" and "investigate and prevent unfair methods of competition" roles are the ones most people are familiar with, but it turns out the FTC has another role – that of providing information to businesses to support these other roles, and it is in this role where the FTC's cybersecurity take place.

For example, the FTC produced a document called the **Standards for Safeguarding Customer Information**. This document applies to the handling of customer information by all financial institutions[1] over which the FTC has rulemaking authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act.

[1] A "financial institution" in this context is An entity is a "financial institution" if its business is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding

The key, and what Al felt was a really good thing, was that it requires financial institutions to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.

The information security program shall:

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer

The elements of the Information Security Program are:

- Designate a qualified individual responsible for overseeing, implementing and enforcing the information security program
- Base information security program on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information
- Design and implement safeguards to control the risks identified through risk assessment – includes requirement to "Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest"
- Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures
- Implement policies and procedures to ensure that personnel are able to enact your information security program
- Oversee service providers
- Evaluate and adjust your information security program in light of the results of the testing and monitoring
- Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control
- Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body

These are all the types of best practices a good information security program should have.

In addition, the FTC has a Data Security Web Site devoted to helping companies protect sensitive personal and company information at https://www.ftc.gov/business-guidance/privacy-security/data-security. This site includes a series of brochures with data security-related information on a range of topics. Some of these topics are (with links to the brochures included):

- **App Developers: Start with Security**
- **Buying or selling debts? Steps for keeping data secure**
- **Careful Connections: Keeping the Internet of Things Secure**
- **Complying with FTC's Health Breach Notification Rule**
- **Consumer Reports: What Information Furnishers Need to Know**

Company Act of 1956, 12 U.S.C. 1843(k), which incorporates activities enumerated by the Federal Reserve Board in 12 CFR 225.28 and 225.86

- **Data Breach Response: A Guide for Business**
- **Digital Copier Data Security: A Guide for Businesses**
- **FTC Safeguards Rule: What Your Business Needs to Know**
- **Health Breach Notification Rule**
- **Health Breach Notification Rule: The Basics for Business**
- **Mobile Health App Developers: FTC Best Practices**
- **Protecting Personal Information: A Guide for Business**
- **Small Business Computer Security Basics**

Al noted the "Digital Copier" brochure, and since the IDS WG is supporting the HCD iTC he decided to see what this brochure had to say. The brochure was written in 2010, but as you'll see it was very advanced in its guidance got the time it was written.

The key points in the Digital Copier Data Security brochure are:

- Digital Copiers are Computers – It is important at the start to note that what this brochure calls a "Digital Copier" is what we would now call a Multi-Function Device – a device that copies, prints, scans, faxes. etc.
    - Require hard disk drives to manage incoming jobs and workloads
    - Hard drive in a digital copier stores data about the documents it copies, prints, scans, faxes or emails that can be stolen from the hard drive – interesting that this was recognized back in 2010 before this fact became common knowledge
- Copiers often are leased, returned, and then leased again or sold
    - Important to know how to secure data that may be retained on a copier hard drive, and what to do with a hard drive when you return a leased copier or dispose of one you own
    - Build in data security for each stage of your digital copier's life-cycle – A very new concept back in 2010
- Before you acquire a copier:
    - Make sure it's included in your organization's information security policies and managed and maintained by your organization's IT staff
    - Employees who have expertise and responsibility for securing your computers and servers also should have responsibility for securing data stored on your digital copiers – What a novel concept - making sure the people who understand security be the ones responsible for implementing security
- When you buy or lease a copier:
    - Evaluate your options for securing the data on the device. Most manufacturers offer data security features with their copiers, either as standard equipment or as optional add-on kits. Typically, these features involve encryption and overwriting
    - Another layer of security that can be added involves the ability to lock the hard drives using a passcode – Al wasn't sure exactly what this meant.
    - Think ahead to how you will dispose of the data that accumulates on the copier over time
- When you use the copier:
    - Take advantage of all its security features. Securely overwrite the entire hard drive at least once a month - Al mentioned that this was an issue throughout his time at Xerox; the Product Security team fought with the Program Teams to get them to enable all the security functions on the device by default at install, with varying results.
    - If your current device doesn't have security features, think about how you will integrate the next device you lease or purchase into your information security plans
    - Plan now for how you will dispose of the copier securely – always a good idea

  - Your organization's IT staff should make sure digital copiers connected to your network are securely integrated to protect against outside intrusions and attacks – something a lot of customers fail to do

- When you finish using the copier:
  - Check with the manufacturer, dealer, or servicing company for options on securing the hard drive. The company may offer services that will remove the hard drive and return it to you, so you can keep it, dispose of it, or destroy it yourself. Others may overwrite the hard drive for you. Typically, these services involve an additional fee, though you may be able to negotiate for a lower cost if you are leasing or buying a new machine – Xerox has such a service where the customer can pay Xerox to take the hard drive from the device when it is returns and dispose of it in a secure manner
  - One cautionary note about removing a hard drive from a digital copier on your own: hard drives in digital copiers often include required firmware that enables the device to operate. Removing and destroying the hard drive without being able to replace the firmware can render the machine inoperable, which may present problems if you lease the device. Also, hard drives aren't always easy to find, and some devices may have more than one. Generally, it is advisable to work with skilled technicians rather than to remove the hard drive on your own – This is an important caution, although customers really shouldn't remove the hard disks on their own unless they have knowledgeable people who know how to do it; otherwise, they should contract out to have it done.

  As indicated above, overall, this was a very complete and insightful HCD security document for something written in 2010.

Another interesting brochure I looked at was a "**Start with Security**" document written in 2015 that compiled lessons learned from previous FTC cases. The key lessons learned were:

- Start with Security
  - Don't collect personal information you don't need
  - Hold on to information only as long as you have a legitimate business need
  - Don't use personal information when it's not necessary

  Three very good best practices

- Control access to data sensibly
  - Restrict access to sensitive data
  - Limit administrative access – restrict access to only those with a need to access the data
- Require secure passwords and authentication
  - Insist on complex and unique passwords
  - Store passwords securely
  - Guard against brute force attacks
  - Protect against authentication bypass – Make sure have proper authentication for access to personal or confidential data
- Store sensitive personal information securely and protect it during transmission
  - Keep sensitive information secure throughout its lifecycle
  - Use industry-tested and accepted methods – such as only use vetted crypto algorithms
  - Ensure proper configuration = make sure set up security features on device properly
- Segment your network and monitor who's trying to get in and out
  - Segment your network
  - Monitor activity on your network – very important step

- Secure remote access to your network
  - Ensure endpoint security
  - Put sensible access limits in place
- Apply sound security practices when developing new products
  - Train your engineers in secure coding – important to also have secure coding guidelines for engineers
  - Follow platform guidelines for security
  - Verify that privacy and security features work
  - Test for common vulnerabilities – also test for any previously found vulnerabilities
- Make sure your service providers implement reasonable security measures
  - Put it in writing
  - Verify compliance

  It is very important to make sure the 3rd Party suppliers implement adequate security measures
- Put procedures in place to keep your security current and address vulnerabilities that may arise
  - Update and patch third-party software – update and patch as soon as new releases are available, especially to fix known vulnerabilities
  - Heed credible security warnings and move quickly to fix them
- Secure paper, physical media, and devices
  - Securely store sensitive files
  - Protect devices that process personal information
  - Keep safety standards in place when data is en-route
  - Dispose of sensitive data securely – At Xerox we had special bins for confidential and proprietary information separate from other recyclable information; the special bin contents were taken and burned.

Al strongly recommended that the attendees look through the various brochures on the FTC Data Security web page; they are actually very informative.

b. Federal Information Security Modernization Act of 2014 (FISMA)

Al did another Google search on the term “cybersecurity laws” and this time Google came up with:

*The three main cybersecurity regulations are **the 1996 Health Insurance Portability and Accountability Act (HIPAA), the 1999 Gramm-Leach-Bliley Act, and the 2002 Homeland Security Act**, which included the Federal Information Security Management Act (FISMA)*

Again, this was a surprise to see these three laws listed. We all have interacted in some form wit HIPAA and Gramm-Leach-Bliley is involved with the financial community. Since Al didn’t really know much about FISMA, he decided to look into FISMA more deeply to see how FISMA is involved with cybersecurity.

The Federal Information Security Modernization Act of 2014 (FISMA) was passed on December 8, 2014. It amends the Federal Information Security Management Act of 2002 to:

- Reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and
- Set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems

So basically, FISMA 2014 essentially just reestablishes (1) DHS administration of the information security policies and practices for the information systems of the various government agencies, and (2) OMB oversite of those information security policies and practices.

FISMA’s main roles are to:

- Provide for the use of automated tools in agencies' information security programs, including for periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents
- Require agencies to include offices of general counsel as recipients of security incident notices
- Require agencies to notify Congress of major security incidents within seven days after there is a reasonable basis to conclude that a major incident has occurred
- Direct agencies to submit an annual report regarding major incidents to OMB, DHS, Congress, and the Comptroller General (GAO). Requires such reports to include: (1) threats and threat actors, vulnerabilities, and impacts; (2) risk assessments of affected systems before, and the status of compliance of the systems at the time of, major incidents; (3) detection, response, and remediation actions; (4) the total number of incidents; and (5) a description of the number of individuals affected by, and the information exposed by, major incidents involving a breach of personally identifiable information
- Authorize GAO to provide technical assistance to agencies and inspectors general, including by testing information security controls and procedures
- Direct FISIC (Federal Information Security Incident Center) to provide agencies with intelligence about cyber threats, vulnerabilities, and incidents for risk assessments
- Require OMB to ensure the development of guidance for: (1) evaluating the effectiveness of information security programs and practices, and (2) determining what constitutes a major incident
- Direct OMB, during the two-year period after enactment of this Act, to include in an annual report to Congress an assessment of the adoption by agencies of continuous diagnostics technologies and other advanced security tools
- Require OMB to ensure that data breach notification policies require agencies, after discovering an unauthorized acquisition or access, to notify: (1) Congress within 30 days, and (2) affected individuals as expeditiously as practicable. Allows the Attorney General, heads of elements of the intelligence community, or the DHS Secretary to delay notice to affected individuals for purposes of law enforcement, the investigations, national security, or security remediation actions
- Require OMB to amend or revise OMB Circular A-130 to eliminate inefficient and wasteful reporting
- Direct the Information Security and Privacy Advisory Board to advise and provide annual reports to DHS

Al singled out the “automated tools” bullet because he felt that pushing automation is the proper way to go and the “FISIC” bullet because FISIC was a new government organization he had not heard of before. However, the general impression of these roles was that FISMA is basically your typical government administrative law and really didn’t offer anything special in terms of cybersecurity.

6. **Actions:** None

Next Steps

The next IDS WG Meeting will be September 7, 2023 at 3:00P ET / 12:00N PT. Main topics will be the latest status of the HCD iTC and HIT and likely a special topic on a TBD topic