IDS WG Meeting Minutes
December 15, 2022

This IDS WG Meeting was started at approximately 3:00 pm ET on December 15, 2022.

Attendees

Graydon Dodson	Lexmark
Matt Glockner	Lexmark
Smith Kennedy	HP
Jeremy Leber	Lexmark
Alan Sukert	
Mike Trent	Xerox
Brian Volkoff	Ricoh
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Special topics on the EU Cyber Resilience Act and a Status Update on the Cybersecurity Executive Order
   - Open Discussion on what IDS should focus on in 2023
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 then presented the first of this week's special topics on the European Union (EU) Cyber Security Act. The slides Al used can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/EU Cyber Resiliency Act.pdf. Given the efforts of the CCRA to agree on terms of mutual recognitional with the EUCC, it is likely that if that happens portions of the CRA may find their way in some form into the CC. Also, since the CRA applies to any product with digital elements that is sold in the EU, that should affect most HCD vendors. That is why understanding what is in the CRA is important.

   The main items covered in the presentation[1] were:

   - The EU Cyber Resilience Act or officially the "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation" was issued on 9/15/22 and addresses the following issues:
     - a) rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products;
     - (b) essential requirements for the design, development and production of products with digital elements;
     - (c) essential requirements for the vulnerability handling processes put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle;
     - (d) rules on market surveillance and enforcement of the above-mentioned rules and requirements

[1] I left out some of the bullets from some of the slides that were mostly "legalese"; see the slides for the full text

Al pointed out that the CRA. Like a lot of the EU cyber-related regulations he has reviewed, places a heavy emphasis on requirements for vulnerability management, much more that corresponding US regulations do.

- The scope of the CRA is:
  - Applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network
  - Does not apply to some products that meet some specific EU regulations
  - Does not apply to products with digital elements developed exclusively for national security or military purposes or to products specifically designed to process classified information

  Key take-aways from this slide were that (1) the CRA applies to any commercial product that connects to a network or device, and that certainly includes HCDs and (2) it does not apply to products with digital elements designed for national security applications. Regarding the latter point, Brian speculated that was because there probably other regulations with stricter requirements that apply to these types of products.
- Some key definitions used in the CRA are:
  - 'product with digital elements': any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately
  - 'critical product with digital elements': a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(2) and whose core functionality is set out in Annex III
  - 'highly critical product with digital elements': a product with digital elements that presents a cybersecurity risk in accordance with the criteria laid down in Article 6(5)
  - 'software': the part of an electronic information system which consists of computer code
  - 'hardware': a physical electronic information system, or parts thereof capable of processing, storing or transmitting of digital data
  - 'significant cybersecurity risk': a cybersecurity risk which, based on its technical characteristics, can be assumed to have a high likelihood of an incident that could lead to a severe negative impact, including by causing considerable material or non-material loss or disruption

  Al noted the definitions of 'software' and 'hardware' used In the CRA are not the standard definitions of the two terms. Al also noted the special definitions for 'critical' and 'highly critical' products with digital elements.
- The essential requirements in the CRA for products with digital elements are:
  - they meet the essential requirements set out in Section 1 of Annex I, under the condition that they are properly installed, maintained, used for their intended purpose or under conditions which can reasonably be foreseen, and, where applicable, updated, and
  - the processes put in place by the manufacturer comply with the essential requirements set out in Section 2 of Annex I

  Al noted that these requirements cover both the development of the product and the role of the manufacturer in assuring the product requirements are met.
- The essential requirements in the CRA for critical products with digital elements are**:**
  - Products with digital elements that belong to a category which is listed in Annex III shall be considered critical products with digital elements. Products which have the core functionality of a category that is listed in Annex III to this Regulation shall be considered as falling into

that category. Categories of critical products with digital elements shall be divided into class I and class II as set out in Annex III, reflecting the level of cybersecurity risk related to these products

- Subject to the conformity assessment procedures referred to in Article 24(2) and (3)

- Al found that it was interesting that the CRA included a list of factors provide a good checklist in determining the level of cybersecurity risk. These factors form a good list that any manufacturer can use internally determine the level of cybersecurity risk.

  The factors that the CRA listed were:

  - (a) the cybersecurity-related functionality of the product with digital elements, and whether the product with digital elements has at least one of following attributes:
    - (i) it is designed to run with elevated privilege or manage privileges;
    - (ii) it has direct or privileged access to networking or computing resources;
    - (iii) it is designed to control access to data or operational technology;
    - (iv) it performs a function critical to trust, in particular security functions such as network control, endpoint security, and network protection
  - (b) the intended use in sensitive environments, including in industrial settings;
  - (c) the intended use of performing critical or sensitive functions, such as processing of personal data;
  - (d) the potential extent of an adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;
  - (e) the extent to which the use of products with digital elements has already caused material or non-material loss or disruption or has given rise to significant concerns in relation to the materialisation of an adverse impact

- The detailed essential requirements for products with digital elements, as defined in Annex 1, are:
  - (1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;
  - (2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;
  - (3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:
    - (a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;
    - (b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;
    - (c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms;
    - (d) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions;
  - (3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

- (e) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimisation of data');
- (f) protect the availability of essential functions, including the resilience against and mitigation of denial-of-service attacks;
- (g) minimise their own negative impact on the availability of services provided by other devices or networks;
- (h) be designed, developed and produced to limit attack surfaces, including external interfaces;
- (i) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;
- (j) provide security related information by recording and/or monitoring relevant internal activity, including the access to or modification of data, services or functions;
- (k) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users

What stands out about these essential requirements is that they are very general in how they are written, meaning it would be very difficult for anyone to evaluate them and determine if they have been met. For example, you can do a vulnerability search to see if any vulnerabilities for the product in question are reported, but for critical or highly critical products is that sufficient to say that there are no known vulnerabilities.

On the positive side these essential requirements do address confidentiality, integrity and availability and things like requirement security by default are important requirements that should be met when they are defined in more specific detail.

What makes the situation worse is that the CRA does not include or point to anything like the CM in the CC that gives evaluator's guidance on how to evaluate these requirements.

They are all solid requirements at a high level, like in the Essential Security Requirements document that the HCD iTC had to produce to get CCDB approval to start the HCD cPP development process.

- The "manufacturing" essential requirements deal with Vulnerability Handling and include the following:
  - (1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;
  - (2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;
  - (3) apply effective and regular tests and reviews of the security of the product with digital elements;
  - (4) once a security update has been made available, publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;
  - (5) put in place and enforce a policy on coordinated vulnerability disclosure;
  - (6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product;

- (7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;
- (8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken

These are solid and reasonable requirements, but like the product one they are general and hard to evaluate to determine in some cases if they have been met. For example, the requirements that talk about "address and remediate vulnerabilities without delay" or "ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner" – how do you define and evaluate what delay time is acceptable or not or what constitutes a "timely manner" where there are no time limits provided for these tasks to be done.

- Annex III has the list of Class 1 and Class II products referenced in the 'product' essential requirements. Slides 11-14 provide the full list and will not be repeated here. But in general Class I products appear to be primarily (1) software-related items such as vulnerability scanners, network management tools, operating systems and software update tools and (2) network devices such as firewalls, routers and microprocessors. Class II products are primarily (1) network devices intended for industrial use and (2) security-related hardware components such as secure elements, Hardware Security Modules and secure cryptoprocessors.
- Article 24 talks about "Continuity Assessment", which is the CRA's term for the evaluation process to determine if the essential requirements have been met. The actual requirement is "Manufacturer shall perform a conformity assessment of the product with digital elements and the processes put in place by the manufacturer to determine whether the essential requirements set out in Annex I are met."

  Article 24 then defines 3 general methods that can be used to perform the Continuity Assessment:

  - (a) the internal control procedure (based on module A) set out in Annex VI; or
  - (b) the EU-type examination procedure (based on module B) set out in Annex VI followed by conformity to EU-type based on internal production control (based on module C) set out in Annex VI; or
  - (c) conformity assessment based on full quality assurance (based on module H) set out in Annex VI

  Note that this requirement calls for a manufacturer self-assessment and not, as is the case in the CC, an independent 3rd Party assessment,

  The problem is there is no Annex VI in the CRA and no definition of what module A, B, C or H are. So, these Continuity Assessment requirements are useless until Annex VI is provided.

  Article 24 also defines a requirement, that in general term (the full requirement is in Slide 16) says that if the manufacturer has not applied EU standards or there is no European cybersecurity certification scheme to do the assessment against, to do the assessment the manufacturer must use methods (b) or (c) above to do the Continuity Assessment.

  Finally, if the product is a critical product, methods (a) or (b) must be used. One final note – Article 24 gives a whole new meeting to the acronym 'SME' – medium sized enterprises
- Al did find an Annex VI about Conformity Assessments in a separate document – the Artificial Intelligence Act (or AI Act). This annex defines the following internal control Conformity Assessment procedure:
  - The provider verifies that the established quality management system is in compliance with the requirements

- The provider examines the information contained in the technical documentation in order to assess the compliance of the AI system with the relevant essential requirements
- The provider also verifies that the design and development process of the AI system and its post-market monitoring is consistent with the technical documentation

This is the standard basic auditing/assessment procedure – verify the requirements are met by examining artifacts to provide evidence the requirements are being met and verifying the define processes/procedures are being followed.

- Article 8 deals with High-Risk AI products. The requirements are defined in very legalese terms, but basically, they are:
  - If the product is compliant with Annex I of the CRA they are compliant with the applicable requirements in the AI Act
  - The Conformity Assessment must be done per the requirements in the AI Act
  - However, critical products as defined by Annex III of the CRA must follow the Continuity Assessment requirements of the CRA
- Article 23 defines the Technical Documentation requirements for the CRA. A key requirement is that the documentation must be kept "during the expected product lifetime or during a period of five years after the placing on the market of a product with digital elements, whichever is shorter." This requirement might imply that from the perspective of the CRA it is expects that products with digital elements will have lifetimes of 5 years or less.
- As Backup AI provided the title and links to all 59 Articles and the 5 Annexes in the CRA, since the CRA website (https://www.european-cyber-resilience-act.com/) provides PDFs for each Article and Annex separately rather that providing a PDF for the entire act.

4. The next special topic was an update on the progress made to implement the US Cybersecurity Executive Order (EO). The slides AI used can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/Cybersecurity Executive Order Update v2.pdf.

   Since the last update in Feb 2022, the following has been accomplished:

   - May 2022: NIST issued "Software Supply Chain Security Guidance Under Executive Order (EO) 14028 Section 4e". This guidance was mentioned in the Feb 2022 update but was actually issued in May.
   - March 7, 2022: OMB released a Statement on "Enhancing The Security Of Federally Procured Software." This statement emphasized two main areas – (1) implementing best practices for implementing the Secure Software Development Framework **(**SSDF) and (2) approaches for ensuring secure software development practices are being followed. This is consistent with NIST's strong focus on the SSDF and requiring vendors developing software as a sole product or as part of hardware to implement and use some type of secure software development process.
   - NIST hosted a workshop on March 23, 2022, on OMB's behalf to inform OMB 4(k) policy implementation based on the above statement.
   - NIST defined additional steps that need to be done to further implement the Cybersecurity EO. The details are in slides 6 and 7, but revolve around the following:
     - **Complete Section 4 Tasks** - Refine OMB guidance to Federal departments and agencies regarding implementation of the criteria developed in response to the EO and complete FAR revisions consistent with the requirements of the EO. Note that the FARs are the clauses that go into Government contracts that actually require the potential bidder to meet specific requirements such as having a secure software development process.
     - **Communicate and Promote Section 4 Deliverables** – (1) Continue tracking and monitoring Section 4 deliverables for their adoption, use, impact, and updating based on experience and

new risks, technologies, and guidance, (2) identify how the criteria and definitions developed under Section 4 can be applied to enhance existing cybersecurity and privacy frameworks such as NIST's Cybersecurity Framework and (3) incorporate Section 4-based criteria and anticipated enforcement mechanisms into maintenance procedures for cybersecurity standards and guidelines.

- **Refine Section 4 Deliverables** – (1) Clarify any ambiguities perceived as hampering enforcement activities, (2) harmonize Section 4 criteria and enforcement mechanisms with the NIST National Initiative for Improving Cybersecurity in Supply Chains broader emphasis on cybersecurity tools, technologies, and guidance focused on the developers and providers of technology and (3) identify and document the implications of Section 4-derived definitions, criteria, and processes for technology workforce requirements and attendant training requirements.

  It was noted that this used the term "harmonize" which is a term that is used extensively in the EU acts and in the EUCC. In this context "harmonize" means to ensure that the Section 4 criteria are consistent with and complement the NIST national initiative mentioned.

- Many of the above actions referenced CISA, which is the other key player in this process besides NIST. CISA (Cybersecurity & Infrastructure Security Agency) was founded in 2018 and is responsible for leading the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure and coordinating the execution of our national cyber defense. There are some additional responsibilities listed in Slide 8.

  CISA's role in implementing the Cybersecurity EO center around the following:

  - "Removing Barriers to Threat Information Sharing Between Government and the Private Sector" by working on cybersecurity-related contract language in the FARs with OMB and developing procedures to ensure timely reporting across Federal agencies of cybersecurity incidents.
  - "Modernizing and Implementing Stronger Cybersecurity Standards across the Federal Government" by things such as supporting efforts to develop a federal cloud security strategy and a cloud service governance framework, help modernize the Federal Risk and Authorization Management Program (FedRAMP), drive adoption of multifactor authentication and encryption for data at-rest and in-transit and work with NIST to develop an initial list of secure software development lifecycle standards for software purchased by the Federal Government and minimum testing requirements for software source code.
  - "Improve Software Supply Chain Security" by helping NIST develop criteria for designating "critical software" and guidelines for required security measures for all software used by the Federal Government and helping the Department of Commerce develop a software bill of materials (SBOM) requirement for products eligible for federal procurement
  - Establish a Cyber Incident Review Board to review actions related to the Federal Government cybersecurity incidents and related supply chain compromise activity and provide recommendations to the Secretary of Homeland Security for improving cybersecurity and incident response practices
  - Create Standardized Playbook for Responding to Cybersecurity Vulnerabilities and Incidents
  - Improve Detection of Cybersecurity Incidents on Federal Government Networks
  - Improve Investigative and Remediation Capabilities by helping develop and issue a policy requiring logging, log retention, and log management across federal agencies (i.e., audit logging)
  - The actions that CISA have actually completed towards implementing its role have been the following:

- Developed the Cloud Security Technical Reference Architecture (TRA) which is a guide for agencies to leverage when migrating to the cloud securely
- Developed a Zero Trust Maturity Model to assist agencies as they implement zero trust architecture that Is based on the foundations of zero trust (Note: **Zero Trust** is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.) to assist agencies in the development of their zero trust strategies and implementation plans
- Published "Applying Zero Trust Principles to Enterprise Mobility" that highlights the need for special consideration for mobile devices and associated enterprise security management capabilities
- Developed two playbooks: one for incident response and one for vulnerability response

  The **Incident Response** Playbook provides a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases as defined in NIST SP 800-61 Rev. 2 and describes the process Federal agencies should follow for confirmed malicious cyber activity for which a major incident has been declared or not yet been reasonably ruled out. Note these cover both known and suspected malicious cyber activity.
- The **Vulnerability Response** Playbook standardizes the high-level process agencies should follow when responding to urgent and high priority vulnerabilities and also addresses vulnerabilities that could be observed by the impacted agency, CISA, industry partners, or others in the related mission space.

5. The last item on the agenda was panned to be a discussion on what the IDS WG should pursue in 2023. However, at the last minute since this is the last meeting in 2022, Al decided to have an open discussion on IDS WG in 2022. The members present indicated that the important thigs IDS accomplished in 2022 were:
   - The HCD cPP v1.0 and HCD SD v1.0 were published in October. IDS was actively involved in helping the HCD iTC develop both documents, both in terms of have IDS members on the HCD iTC and in terms of providing inputs to the HCD iTC.
   - Efforts were initiated in 2022 to try to connect what the IDS WG is doing more with the efforts of the IPP WG and the PWG as a whole, so that the two WGs are no longer "stovepipes" but rather parts of an integrated PWG. This includes tasks like reviewing the PWG security web page to align it with the HCD cPP and to include IDS activities related to security on the web page. This integration work is in progress but "is not there yet".
   - Al's efforts working with Paul Tykodi to marry the IPP work on 3D printing with the IDS work on Common Criteria. This effort resulted in Al presenting a paper at the ASTM ISAM Conference on applying Common Criteria to security certifications of the Digital Thread for Additive Manufacturing.

   The discussion on 2023 IDS activities will be done at the first IDS WG Meeting in 2023 on Jan 12th.
6. **Actions:** None

Next Steps

- The next IDS WG Meeting will be January 12, 2023 at 3:00P ET / 12:00N PT. Main topics will be a special topic (likely the EU Artificial Intelligence Act) and a discussion on what IDS should do in 2023.
- The next PWG Face to Face Meetings will be February 7-9, 2023. The IDS Session will likely be on February 9th from 10A – 12N ET.