IDS WG Meeting Minutes
April 28, 2022

This IDS WG Meeting was started at approximately 3:00 pm ET on April 28, 2022.

Attendees

Graydon Dodson	Lexmark
Erin Huber	Xerox
Jeremy Leber	Lexmark
Alan Sukert	
Bill Wagner	TIC
Steve Young	Canon

Agenda Items

1. The topics to be covered during this meeting were:
   - Review of the HCD iTC Meetings since our last IDS WG Meeting on 3/31/22
   - Presentation by Al Sukert on the NIST Framework for Improving Critical Infrastructure Cybersecurity
   - 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 then provided a summary of what was covered at the HCD iTC Meetings since the last IDS Workgroup meeting on 3/31/22.
   - Most of the time spent at the HCD iTC meetings since the last IDS WG Meeting was spent finalizing the new FPT_WIPE_EXT SFR and its associated Assurance Activities (AAs). Specifically, the HCD iTC work to address comments to the FPT_WIPE_EXT SFR and AAs from the Korean Scheme and, more importantly, from NIAP. It is important that the HCD iTC get buy-in from NIAP for the HCD cPP and for this SFR because the HCD iTC wants any HCD that is certified against the HCD cPP/SD to be accepted by NIAP so it can be included on the NIAP Product Compliant List (PCL). That will allow that HCD to be sold to the US Government.

     The main work over the last two weeks in the HCD iTC was to address the NIAP comments against the FPT_WIPE_EXT SFR and AAs. The NIAP comments centered on x issues:

     - Concern that the "*[**assignment:** media-specific method(s)]*" selection entry in the FPT_WIPE_EXT SFR was too broad and needed to be more specific in terms of the methods specified
     - Whether the FDP_RIP.1/Overwrite SFR applied to wear-leveling devices or not (i.e., was overwrite only allowed for non-wear-leveling devices)
     - Making sure the FPT_WIPE_EXT SFR aligned with FCS_CKM.4
     - Documentation of data on the device should specify encrypted documents

     To address the NIAP comments the following changes were made to the FPT_WIPE_EXT SFR and AAs (changed wording is in bolded text):

     - The wording of the FDP_RIP.1/Overwrite SFR was modified as follows to clarify that it applied to both wear-leveling and non-wear-leveling devices -- FDP_RIP.1.1/Overwrite Refinement: The TSF shall ensure that any previous information content stored on a **[selection: wear-leveled storage device, non-wear-leveled storage device]** of a resource is made unavailable [selection: by overwriting data, by destroying its cryptographic key] upon the deallocation of the resource from the following objects: D.USER.DOC.

Bill brought up that this change contradicts the proposed change to cPP Section 3.5.6 that adds the wording "This objective may only be included in STs for TOEs that do not store any D.USER.DOC data on wear-leveling storage devices (e.g., SSDs)." Al indicated he would bring this issue up at the next HCD iTC Meeting.

- Changed the "*[**assignment:** media-specific method(s)]*" selection entry in the FPT_WIPE_EXT SFR to two new specific method entries:
  - *media specific eMMC method,*
  - *media specific ATA erase method*
- Modified AA Test 3 to be consistent with the above change as follows:

  Test 3: [*Conditional: If a media-specific method or block erase is selected*] Using a debug log or special tooling that the developer shall provide, the evaluator shall verify that the media-specific method or block erase command is executed.

  This test verifies the execution of the media-specific method or block erase command.
- Added the following to the TSS AA:
  The evaluator shall ensure the storage medium(s) subject to overwrite are identified and the storage medium(s) leverage functionality that matches the selection on wear-leveling.

  The evaluator shall examine the TSS to ensure that the TSS describes the type(s) of overwrite (e.g., single overwrite with zeros) of D.USER.DOC that the TOE performs.
- Add the following to the Guidance AA:

  The evaluator shall check to ensure that the operational guidance describes the type(s) of overwrite (e.g., single overwrite with zeros) of user document data that the TOE performs.
- Removed the following from the TSS AA:

  The evaluator shall review the types of storage devices and determine that all wear-leveling types of storage (e.g., SSDs) are not cleared solely by an "overwrite" method, the TSS documents that D.USER or D.TSF could remain on the device.

The only concern at this point is that the iTC has not received any feedback on the FPT_WIPE_EXT SFR and AAs from the Japanese Scheme. Buy-in from the Japanese Scheme is needed to allow the SFR and AAs to get into the Final Draft of the cPP and SD. Kwangwoo Lee is working on getting Japanese Scheme feedback on the FPT_WIPE_EXT SFR and AAs.

- Al then briefly went over the latest HCD iTC schedule status. Currently all comments against the 2nd Public Drafts of both the HCD cPP and HCD SD have been addressed by the HCD iTC. The current HCD iTC Workplan has the following key milestones
  - Submit Final Draft of HCD cPP and HCD SD: 5/16
  - Review HCD cPP/SD Final Drafts: 5/17 – 6/20
  - Review comments against HCD cPP/SD Final Drafts and update documents: 6/21 – 6/30
  - Publish HCD cPP v1.0 and HCD SD v1.0: 7/5/22

  Right now, the HCD iTC is on-track for the Final Drafts of both the HCD cPP and HCD SD to be submitted for public review on 7/16 subject to any last-minute issues. That means as of today the HCD iTC is on-track for publishing HCD cPP and HCD SD v1.0 around the beginning of July 2022. However, as Ira had mentioned at a previous meeting most of the comments come against the Final Draft (because it is the first time many reviewers read the documents) so we will have to see what comments come in against the Final Draft and how that affects the final publishing data.

Al mentioned that the fact the HCD iTC is close to publishing the Final Drafts of the HCD cPP and SD means the iTC is entering a new phase, given that it is 2-1/2 months from publishing the documents. The iTC has to start planning for two things:

- It has to start to set up procedures and membership for the HCD iTC Interpretation Team (we are calling it the "HIT Team"). The HIT Team essentially is a subset of the full HCD iTC that is charged with maintaining the current published versions of the HCD cPP and HCD SD. Specifically, the HIT Team is responsible for addressing questions and any comments against the current published versions of the HCD cPP and HCD SD and then determine and implement any resolutions to the questions and comments (e.g., implement a change to the current version of the document or recommend a change to a future version of the document or recommend no change to the document).
- It has to start planning for future updates of the HCD cPP and HCD SD. The HCD iTC has to address questions like what will be intervals between major and minor updates and what will go into the next update of the cPP and SD.

It means that what will be covered in future HCD iTC meetings will start to change over the next couple of months.

4. Al then went through a presentation he put together on the NIST Framework for Improving Critical Infrastructure Cybersecurity (commonly called the NIST Cybersecurity Framework); https://www.nist.gov/cyberframework provides a link to the documentation for the NIST Cybersecurity Framework. The presentation slides are located at https://ftp.pwg.org/pub/pwg/ids/Presentation/NIST Cybersecurity Framework.pdf.

- The current version of the NIST Cybersecurity Framework is Version 1,1 issued April 16, 2018. The NIST Cybersecurity Framework is a direct result of the Cybersecurity Enhancement Act of 2014 that required NIST to:
  - Facilitate and support the development of" cybersecurity risk frameworks and
  - Identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks."
- Critical infrastructure, as defined by the Patriot Act, are "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."
- The NIST Cybersecurity Framework discusses that based on this definition of critical infrastructure DHS has defined 16 Critical Infrastructure Sectors that perform functions that are supported by the broad category of technology, including information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), and connected devices more generally, including the Internet of Things (IoT). While many of these sectors – e.g., Energy, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials & Waste, Transportation Systems – are what you'd expect; some are not. For example, one of the Sectors is Commercial Facilities which includes things like shopping malls. If you think about it that makes sense, since malls are a convenient terrorist target to inflict maximum damage to civilians. Food and Agriculture is another sector that would seem odd but a disruption in food supplies can have a detrimental effect on economies and many other factors.
- The goals of the NIST Cybersecurity Framework are to provide a common taxonomy and mechanism for organizations to:
  - Describe their current cybersecurity posture
  - Describe their target state for cybersecurity

  - Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
  - Assess progress toward the target state
  - Communicate among internal and external stakeholders about cybersecurity risk
- The NIST Cybersecurity Framework is comprised of three basic components:
  - Framework Core - a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Framework Core is composed of the following:
    - **Functions** which organize basic cybersecurity activities at their highest level. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities
    - **Categories** which are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities
    - **Subcategories** which further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category
    - **Informative References** are specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory
  - 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).
  - Framework Profile (“Profile”): A 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
- The 5 Framework Core Functions are:
  - **Identify** – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
  - **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services
  - **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event
  - **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident
  - **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
- The four Framework Implementation Tiers are defined as follows:

  Tier 1: Partial

  - *Risk Management Process* – Organizational cybersecurity risk management practices are not formalized, and risk is managed in an *ad hoc* and sometimes reactive manner. Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements
  - *Integrated Risk Management Program* – There is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside

sources. The organization may not have processes that enable cybersecurity information to be shared within the organization

- *External Participation* – The organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization does not collaborate with or receive information (e.g., threat intelligence, best practices, technologies) from other entities (e.g., buyers, suppliers, dependencies, dependents, ISAOs, researchers, governments), nor does it share information. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses

Tier 2: Risk Informed

- *Risk Management Process* – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements
- *Integrated Risk Management Program* – There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring
- *External Participation* – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks

Tier 3: Repeatable

- *Risk Management Process* – The organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape
- *Integrated Risk Management Program* – There is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors cybersecurity risk of organizational assets. Senior cybersecurity and non-cybersecurity executives communicate regularly regarding cybersecurity risk.
  Senior executives ensure consideration of cybersecurity through all lines of operation in the organization
- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. It collaborates with and receives information from other entities regularly that complements internally generated information, and shares information with other entities. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses. Additionally, it usually acts formally upon those risks, including mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring

Tier 4: Adaptive

- *Risk Management Process* – The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators
- *Integrated Risk Management Program* – There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. The relationship between cybersecurity risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor cybersecurity risk in the same context as financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities and continuous awareness of activities their systems and networks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated
- *External Participation* - The organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. It receives, generates, and reviews prioritized information that informs continuous analysis of its risks as the threat and technology landscapes evolve. The organization shares that information internally and externally with other collaborators. The organization uses real-time or near real-time information to understand and consistently act upon cyber supply chain risks associated with the products and services it provides and that it uses

Al mentioned that Tier 1 is like Ad Hoc – no cybersecurity practices and procedures and limited awareness of the use of risk management to address cybersecurity. Tier 2 is where cybersecurity practices and use of risk management are established but not organization-wide. Tier 3 is where use of cybersecurity practices and procedures and risk management are established organization-wide and everyone buys-in to their use and understands their role. Tier 4 is where Tier 3 is expanded to include use of lessons learned, continuous improvement and data driven methodologies.

- Framework Profiles help to:
  - Align Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization
  - Establish a roadmap for reducing cybersecurity risk that is well aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects risk management priorities
  - Describe the current state or the desired target state of specific cybersecurity activities
  - Use a Current Profile to indicate the cybersecurity outcomes that are currently being achieved
  - Use a Target Profile to indicate the outcomes needed to achieve the desired cybersecurity risk management goals
  - Use comparison of Profiles (e.g., the Current Profile and Target Profile) to help reveal gaps to be addressed to meet cybersecurity risk management objectives
- Al went through the Categories of each of the five Device Framework Core Functions and then quickly went through the Subcategories for each Category. Some of the key points from the discussion are discussed below (Note -the notes below do not cover all the Categories and Subcategories in the NIST Cybersecurity Framework; only the ones Al commented on during his presentation at the meeting. The full presentation has all the Categories/Subcategories for each Function):

- The Categories for the **Identify** Function are:
  - **Asset Management:** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy
  - **Business Environment:** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions
  - **Governance:** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk
  - **Risk Assessment:** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals
  - **Risk Management Strategy:** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions
  - **Supply Chain Risk Management:** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks
- The subcategories for the **Risk Assessment** category are:
  - Asset vulnerabilities are identified and documented
  - Cyber threat intelligence is received from information sharing forums and sources
  - Threats, both internal and external, are identified and documented
  - Potential business impacts and likelihoods are identified
  - Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
  - Risk responses are identified and prioritized

  Al pointed out that it was important that this included the use of threats, vulnerabilities, likelihoods, and impacts to determine the risk.
- The subcategories for the **Supply Chain Risk Management** category are:
  - Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
  - Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
  - Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan
  - Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations
  - Response and recovery planning and testing are conducted with suppliers and third-party providers

  Al pointed out the connection between this category and the Supply Chain requirements in the Cybersecurity Executive Order from 2021. In fact, much of what are in the NIST documents that are coming out of the Cybersecurity Executive Order from 2021 are based on the NIST Cybersecurity Framework.
- The Categories for the **Protect** Function are:

  - **Identity Management, Authentication and Access Control**: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions
  - **Awareness and Training**: The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements
  - **Data Security**: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information
  - **Information Protection Processes and Procedures**: Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets
  - **Maintenance**: Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures

    Al noted that Maintenance in this context was strictly hardware maintenance and had nothing to do with software maintenance.
  - **Protective Technology**: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements

    Al noted that this subcategory was also mostly focused on hardware rather than software.

- The subcategories for the **Identity Management, Authentication and Access Control** category are:
  - Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
  - Physical access to assets is managed and protected
  - Remote access is managed
  - Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
  - Network integrity is protected (e.g., network segregation, network segmentation)
  - Identities are proofed and bound to credentials and asserted in interactions
  - Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)

  Al stated that these were the type of subcategories one would expect for identification, authentication and authorization, although they are stated in a different way than we state then in the HCD cPP.

- The subcategories for the **Awareness and Training** category are:
  - All users are informed and trained
  - Privileged users understand their roles and responsibilities
  - Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
  - Senior executives understand their roles and responsibilities
  - Physical and cybersecurity personnel understand their roles and responsibilities

  Al indicated that these are the same type of assumptions that we include in the HCD cPP – those users and administrators are properly trained.

- The subcategories for the **Data Security** category are:
    - Data-at-rest is protected
    - Data-in-transit is protected
    - Assets are formally managed throughout removal, transfers, and disposition
    - Adequate capacity to ensure availability is maintained
    - Protections against data leaks are implemented
    - Integrity checking mechanisms are used to verify software, firmware, and information integrity
    - The development and testing environment(s) are separate from the production environment
    - Integrity checking mechanisms are used to verify hardware integrity

  Al pointed out that these are stated very simply compared to how they are stated in the HCD cPP. It was also pointed out the inclusion of the “Integrity checking mechanisms are used to verify hardware integrity” subcategory which the HCD iTC spent a lot of time working on determining the requirements for integrity verification on the Chains of Trust during the Boot process.

- The subcategories for the **Information Protection Processes and Procedures** category are:
    - A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)
    - A System Development Life Cycle to manage systems is implemented
    - Configuration change control processes are in place
    - Backups of information are conducted, maintained, and tested
    - Policy and regulations regarding the physical operating environment for organizational assets are met
    - Data is destroyed according to policy
    - Protection processes are improved
    - Effectiveness of protection technologies is shared
    - Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
    - Response and recovery plans are tested
    - Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
    - A vulnerability management plan is developed and implemented

  It was pointed out the inclusion of a subcategory for a System Development Life Cycle, although Al wished the subcategory had been for a Secure Development Life Cycle rather than just a System Development Life Cycle.

- The Categories for the **Detect** Function are:
    - **Anomalies and Events**: Anomalous activity is detected and the potential impact of events is understood
    - **Security Continuous Monitoring**: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures
    - **Detection Processes**: Detection processes and procedures are maintained and tested to ensure awareness of anomalous events
- The subcategories for the **Security Continuous Monitoring** category are:

  - The network is monitored to detect potential cybersecurity events
  - The physical environment is monitored to detect potential cybersecurity events
  - Personnel activity is monitored to detect potential cybersecurity events
  - Malicious code is detected
  - Unauthorized mobile code is detected
  - External service provider activity is monitored to detect potential cybersecurity events
  - Monitoring for unauthorized personnel, connections, devices, and software is performed
  - Vulnerability scans are performed

  It was pointed this subcategory includes not only monitoring the network and detection of malware but vulnerability scanning which was much more in vogue in 2018 that it is now is 2022.

- The subcategories for the **Detection Processes** category are:
  - Roles and responsibilities for detection are well defined to ensure accountability
  - Detection activities comply with all applicable requirements
  - Detection processes are tested
  - Event detection information is communicated
  - Detection processes are continuously improved

  Al indicated that it was important that they included the subcategory here that the detection processed should be tested.

- The Categories for the **Respond** Function are:
  - **Analysis**: Analysis is conducted to ensure effective response and support recovery activities
  - **Mitigation**: Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident
  - **Improvements**: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities

  As a general comment on all the categories, the subcategories essentially revolve around (1) do the analysis using forensics, (2) mitigate the incidents, and (3) develop response plans and lessons learned.

- The Categories for the **Recover** Function are:
  - **Recovery Planning**: Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents
  - **Improvements**: Recovery planning and processes are improved by incorporating lessons learned into future activities
  - **Communications**: Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors)

  Similarly, as with the Respond Function, the three categories essentially involve execute the recovery plan after an incident, make sure you update recovery plans based on lessons learned and mitigate the PR and “political” fallout from the incident.

- Finally, the NIST Cybersecurity Framework document discussed how the Framework could be used. The main uses mentioned were:
  - Compare an organization’s current cybersecurity activities with those outlined in the Framework Core

- Develop a current profile based on the Core Functions, Categories and Subcategories and see where the gaps are against the Core
- Establish or Improve a Cybersecurity Program
- Develop a current profile, do a risk assessment, create a target profile and determine gaps and implement action plans
- Communicating Cybersecurity Requirements with Stakeholders
- Provides a connection to Supply Chain Risk Management and thus to the Cybersecurity Executive Order
- Could be used to compare bidders in purchase decisions as a bid criterion
- The actual NIST Cybersecurity Framework document does make a case where this framework could be used to determine where a cybersecurity program is going too far with respect to privacy and civil liberty issues

It was the last use that was surprising in that it was actually mentioned in the document.

5. **Actions:** None

Next Steps

- The next IDS WG Meeting will be May 12, 2022 at 3:00P ET / 12:00N PT. Main topics will be review of the 5/2 and 5/9 HCD iTC Meetings, possibly a special topic and preparation for the IDS Face-to-Face Meeting on May 19th.
- The IDS Face-to-Face Meeting that is part of the May Virtual PWG/OpenPrinting Meeting will be on May 19th at 12:45 PM ET.