The Printer Working Group

Imaging Device Security

February 9, 2023

PWG February 2023 Virtual Face-to-Face

Agenda

Please Note: This PWG IDS Meeting is Being Recorded

When	What
10:00 – 10:05	Introductions, Agenda review
10:05 – 10:45	Discuss status of HCD iTC and plans for future HCD cPP/HCD SD releases
10:45 – 11:25	Cybersecurity in the US
11:25 – 11:30	HCD Security Guidelines v1.0 Status
11:30 – 11:55	TCG/IETF Liaison Reports
11:55 – 12:00	Wrap Up / Next Steps

Antitrust and Intellectual Property Policies

"This meeting is conducted under the rules of the PWG Antitrust, IP and Patent policies".

- Refer to the Antitrust, IP and Patent statements in the plenary slides

Officers

- Chair:
  - Alan Sukert
- Vice-Chair:
  - TBD
- Secretary:
  - Alan Sukert
- Document Editor:
  - Ira McDonald (High North) – HCD Security Guidelines

HCD international Technical Community (iTC) Status

HCD international Technical Community (iTC) Status

- Since last IDS F2F on November 17, 2022 HCD iTC meetings have been held on:
  - November 21st
  - December 5th, 19th
  - January 9th, 30th

  NOTE: Since publishing the HCD cPP v1.0 and HCD SD v1.0 in Oct 2022 the HCD iTC has gone to meeting every other week
- Current focus is on developing a release plan for future versions of the HCD cPP and HCD SD

HCD cPP/SD v1.0 Status

- Version 1.0 of both documents published on October 31, 2022
- Awaiting Position Statements from NIAP (US), ITSCC (Korea), JISEC (Japan) and Canadian Scheme
  - NIAP is currently reviewing the HCD cPP
  - As of Jan 29th had no status on ITSCC or JISEC
  - Canadian Scheme indicated that it may have a vendor that wants to certify an HCD against the published HCD cPP / HCD SD as soon as possible
- Created a list of the major changes between the approved HCD PP and the published HCD cPP / SD
  - Found grammatical or minor text errors in the HCD cPP / SD that will require an Errata

HCD cPP/SD
HCD Interpretation Team (HIT) Status

- HIT initial membership team formed with 7 members
  - Have designated a HIT Lead and HIT Deputy Lead
  - Current membership is from HCD vendors and Evaluation Lab
  - NIAP may provide a member
  - Goal is to have a maximum of 10 members on the HIT
- HIT procedures under development
  - Draft 4 of procedures ready for HIT membership review
  - Will use GitHub for documenting Requests for Interpretation (RfIs) and for creating and tracking changes to HCD cPP v1.0 and HCD SD v1.0 for approved RFIs
  - Will have to maintain two baselines for approved RfIs requiring changes to either the HCD cPP v1.0 or HCD SD v1.0:
    - One baseline for the approved changes to either document that are also approved by NIAP as NIAP Technical Decisions (TDs)
    - One baseline for the approved changes to either document that are not approved by NIAP
- Looking to have HIT implemented by end of February 2023

HCD cPP/SD
HCD Interpretation Team (HIT) Process

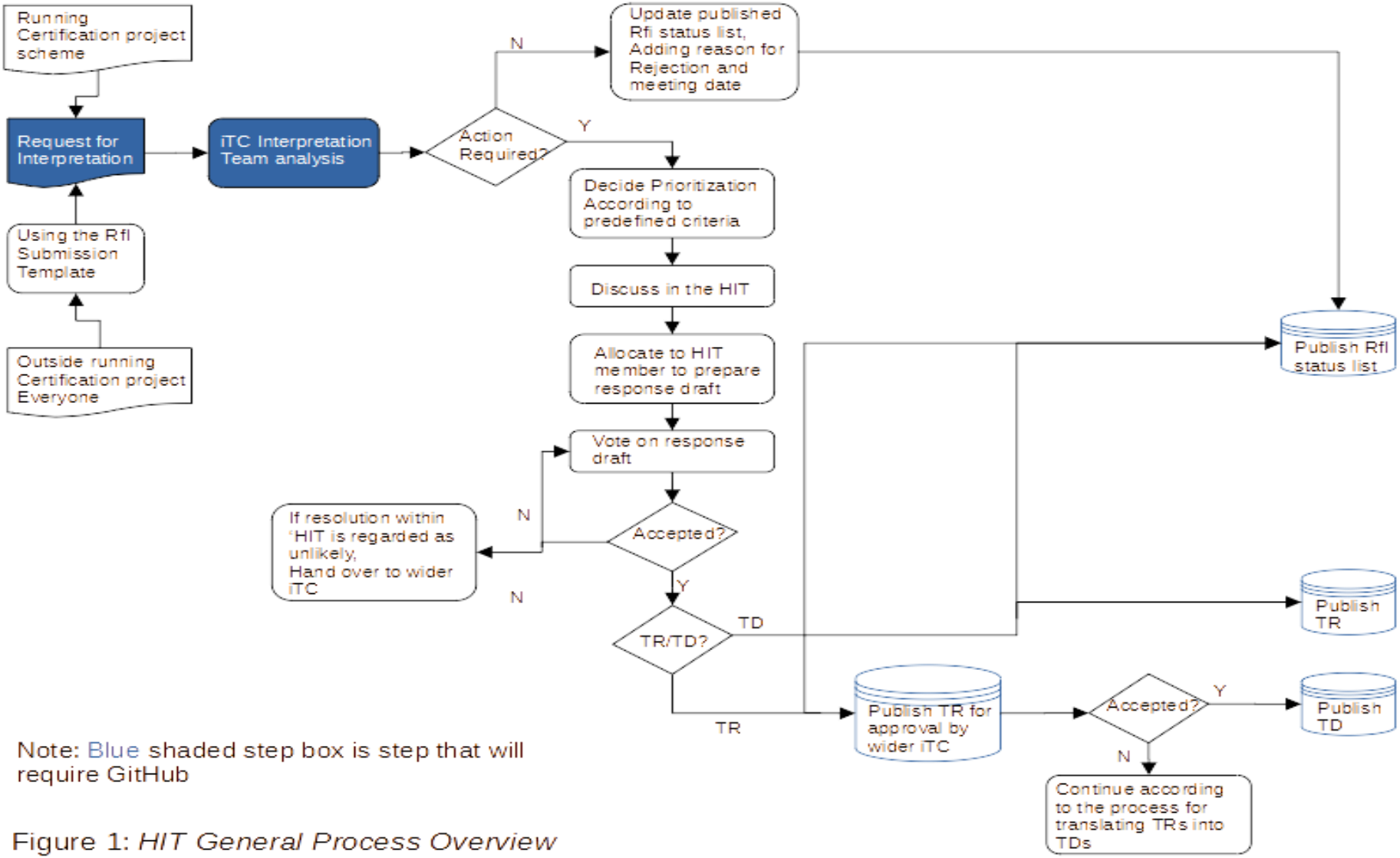

Figure 1: *HIT General Process Overview*

HCD cPP/SD
Current Parking Lot Issues – HCD cPP

- Addressing hardware-based Roots of Trust stored in mutable memory as well as immutable memory
- Clarification that the Secure Boot SFR only requires verification of firmware/software that is stored in mutable memory at boot time and does not require verification of firmware/software stored in immutable memory
- Comments that require implementation of TLS 1.3 to resolve
- Support for NTP
- Addition of 3 TLS cipher suites required per NIAP Technical Decision TD442
- Add a selection in FCS_COP.1/SigGen for IKEv1 RSA schemes
- Removal of support for:
  - TLS 1.1
  - SHA-1 support
  - Cipher suites with RSA Key Generation with keys < 2048 bits
  - All RSA and DHE Key Exchanges

HCD cPP/SD
Current Parking Lot Issues – HCD SD

- Correcting TSS Assurance Activities for SFR FCS_CKM.4 Key Destruction
- Correcting Test 2 for SFR FCS_CKM.4 Key Destruction to provide a valid test for where the data read operation would fail
- Clarification of TSS Assurance Activities for SFR FIA_X509_EXT.2 X.509 Certificate Authentication

HCD iTC
Issues Post-Version 1.0 – Release Plan

- Developing release plan for future updates of the HCD cPP and HCD SD
  - Will have major and minor releases
  - First update to HCD cPP and HCD SD will likely be "Errata" releases
  - Timeframe for releases:
    - per other iTCs
    - TimNo specific rules for the timeframe of its ND cPP/SD releasese frame between minor releases – looking at possibly every 12 -18 months maximum if no "emergency" releases require an earlier release time
    - Time frame between major releases – Need to decide if based on calendar time (e.g., every 2 or 3 years), number of minor releases (e.g., a major release every 4 minor releases), volume of changes, number of new requirements/features added, a combination of all of these factors or something else
  - What goes into a major or minor release – could be any or all of:
    - TDs approved by the HIT or TRs from the HIT that are approved by the full HCD iTC
    - Applicable NIAP TDs
    - Changes resulting from syncing with ND and FDE cPPs/SDs
    - Requests from Schemes, especially JISEC, ITSCC and NIAP
    - Response to new technologies, new crypto algorithms, new or updated standards or NIST SPs
    - New or updated requirements/features

  Key is to maintain backwards compatibility and maintain functionality with previous release

HCD iTC
Issues Post-Version 1.0 – CNSA 2.0

- Commercial National Security Algorithm (CNSA) 2.0 released by NSA Sep 2022
- Addresses problem that future deployment of a cryptanalytically relevant quantum computer (CRQC) would break public-key systems still used today
- Need to plan, prepare, and budget for an effective transition to quantum-resistant (QR) algorithms, to assure continued protection of National Security Systems (NSS) and related assets
- Is an update to CNSA 1.0 Algorithms
- Applies to all NSS use of public cryptographic algorithms (as opposed to algorithms NSA developed), including those on all unclassified and classified NSS
- Using any cryptographic algorithms the National Manager did not approve is generally not allowed, and requires a waiver specific to the algorithm, implementation, and use case
- Per CNSSP 11, software and hardware providing cryptographic services require NIAP or NSA validation in addition to meeting the requirements of the appropriate version of CNSA

Commercial National Security Algorithm (CNSA) Suite 1.0 Algorithms

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

Commercial National Security Algorithm (CNSA) Suite 2.0 Algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels SHA256/192 recommended
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels

Transitioning to CNSA Suite 2.0

- The timing of the transition depends on the proliferation of standards-based implementations
- NSA expects the transition to QR algorithms for NSS to be complete by 2035 in line with NSM-10.
- NSA urges vendors and NSS owners and operators to make every effort to meet this deadline.
- Where feasible, NSS owners and operators will be required to prefer CNSA 2.0 algorithms when configuring systems during the transition period.
- When appropriate, use of CNSA 2.0 algorithms will be mandatory in classes of commercial products within NSS, while reserving the option to allow other algorithms in specialized use cases

Detailed NIAP Transition Plan for CNSA Suite 2.0

- Currently all NIAP PPs must have CNSA 1.0 algorithms
- Will add SHA-512 to all NIAP PPs
- Will require either CNSA 1.0 or CNSA 2.0 be mandatory on all NIAP PPs
- Will implement CNSA asymmetric algorithms for software/firmware signing per following
  - LMS – 1H 2023
  - XMSS – 2H 2023
- Will implement following Key Establishment CNSA 2.0 algorithms in all NIAP PPs when they are standardized and all relevant Assurance Activities have been defined and agreed upon:
  - CRYSTALS - Kyber
  - CRYSTALS – Dilithium (used for Digital Signatures)
- Will deprecate CNSA 1.0 in 2030 – 2033 timeframe
- No current timeline established to make CNSA 2.0 mandatory
  - Will make use of CNSA 2.0 mandatory to be listed on PCL at some point
- Will work with vendors to help try to meet NSA schedule
- Will discuss with CCRA and engage with iTCs how best to integrate CNSA 2.0 into cPPs

HCD cPP/SD Content Post-Version 1.0 Likely V1.1 Content

- Inclusion of support for TLS 1.3 and deprecation of TLS 1.1
- Inclusion of NTP
- Inclusion of AVA_VAN and ALC_FLR.*
  - Is included in ND cPP v3.0 currently in final review
- Initial implementation of CNSA 2.0 algorithms
  - Inclusion of SHA-384 and SHA-512 and inclusion of LMS as an option likely first steps
- Sync with ND cPP/SD v3.0 to be published sometime in 1Q 2023
  - Incorporate NIAP SSH Package
  - Comparisons of HCD cPP / HCD SD with ND cPP / ND SD v3.0 counterparts revealed other changes that should be looked at by HCD iTC for inclusion
- Changes due to any approved RfIs to HCD cPP/SD v1.0
  - Will have to decide if only include changes approved by NIAP
- Updates to CC2022 published in November 2022
  - Comparison of CC2022 Part 2 to CC v3.1R5 revealed several changes that should be looked at by the HCD iTC for inclusion
- Changes due to requests from JISEC, ITSCC or NIAP (Canada also?)

HCD cPP/SD Content Post-Version 1.0 Potential for Inclusion in v1.1 or Later

- **Full implementation of CNSA 2.0**
- **Support for new crypto algorithms**
- **NIAP IPsec Package**
- **Updates due to changes from other ISO, FIPS or NIST Standards/Guidelines, NIAP TDs**
- **Expand to address 3D printing**
- Support for Wi-Fi and maybe Bluetooth
- Support for Security Information and Event Monitoring (SIEM) and related systems
- Any new CCDB Crypto WG or CCUF Crypto WG Packages
- Support for SNMPv3
- Support for NFC
- Indirect updates based on new technologies or customer requests

HCD iTC Status
Key Next Steps

- Implement the HIT for maintaining HCD cPP/SD v1.0
- Agree on the HCD cPP/HCD SD release plan
- Determine the content for and then create the next HCD cPP/SD release (v1.1)
- Ensure that the HCD iTC continues to be fully engaged now that HCD cPP v1.0 and HCD SD v1.0 have been published

HCD iTC Status
Final Lessons Learned from v1.0 (My Take)

- Requires a dedicated group of editors to get a cPP or SD version published
- We were lax in creating and monitoring our Work Plan for the HCD cPP/SD v1.0 development; need to do better for future versions of these documents
- Work Plans and schedules need to be realistic
- Tracking the changes for v1.0 was a tedious manual process – it needs to be more automated for future releases

Cybersecurity in the United States

Cybersecurity in the US General Observations

- Current cybersecurity activities with the US Government are based on four key sources – the Federal Information Security Modernization Act of 2014, the Cybersecurity Enactment Act of 2014, the Cybersecurity Enactment Act of 2015 and the 2021 Executive Order on Improving the Nation's Cybersecurity
  - Are other laws that update or expand on these four laws
- Cybersecurity laws apply only to what the government agencies must do; the agencies like NIST are chartered to provide standards and guidelines to implement the cybersecurity laws
- US Government cybersecurity activities are spread over multiple government agencies – NIST, CISA, DHS
- There is a large number of cybersecurity frameworks developed by and for US Government Agencies and cybersecurity frameworks developed for specific industries or industry groups

Federal Information Security Modernization Act of 2014

- Codifies the Department of Homeland Security's role in administering the implementation of information security policies for federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting OMB in developing those policies
- Provides the Department authority to develop and oversee the implementation of binding operational directives to other agencies, in coordination and consistent with OMB policies and practices
- Authorizes DHS to provide operational and technical assistance to other federal Executive Branch civilian agencies at the agency's request
- Places the federal information security incident center within DHS by law
- Authorizes DHS technology deployments to other agencies' networks (upon those agencies' request)
- Directs OMB to revise policies regarding notification of individuals affected by federal agency data breaches
- Requires agencies to report major information security incidents as well as data breaches to Congress as they occur and annually
- Simplifies existing FISMA reporting to eliminate inefficient or wasteful reporting while adding new reporting requirements for major information security incidents

Executive Order on Improving the Nation's Cybersecurity - 2021

Issued May 12, 2021

Key Areas Covered by this Executive Order:

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

Cybersecurity Enactment Act of 2014

- NIST shall facilitate and support on an ongoing basis the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure
- Heads of the applicable federal agencies and departments shall develop and update every 4 years a Federal cybersecurity research and development strategic plan
- Director of the National Science Foundation shall support research that develops, evaluates, disseminates, and integrates new cybersecurity practices and concepts into the core curriculum of computer science programs and of other programs and develops new models for professional development of faculty in cybersecurity education, including secure coding development
- NIST shall, as necessary, develop and revise security automation standards, associated reference materials (including protocols), and checklists that minimize the security risks associated with each information technology hardware or software system and security tool that is, or is likely to become, widely used within the Federal Government
- OPM shall support competitions and challenges to identify, develop, and recruit talented individuals to perform duties relating to the security of information technology in Federal, State, local, and tribal government agencies, and the private sector
- NIST shall continue to coordinate a national cybersecurity awareness and education program
- Shall ensure coordination of Federal agencies engaged in the development of international technical standards related to information system security
- Shall continue to develop and encourage the implementation of a comprehensive strategy for the use and adoption of cloud computing services by the Federal Government
- Shall continue a program to support the development of voluntary and cost-effective technical standards, metrology, testbeds, and conformance criteria

Cybersecurity Enactment Act of 2015

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

Cybersecurity in the US
NIST

- Develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public
- Some NIST cybersecurity assignments are defined by federal statutes, executive orders and policies. For example, the Office of Management and Budget (OMB) mandates that all federal agencies implement NIST's cybersecurity standards and guidance for non-national security systems
- Activities also are driven by the needs of U.S. industry and the broader public
- Advances understanding and improves the management of privacy risks, some of which relate directly to cybersecurity
- Priority areas to which NIST contributes – and plans to focus more on – include cryptography, education and workforce, emerging technologies, risk management, identity and access management, measurements, privacy, trustworthy networks and trustworthy platforms

Cybersecurity in the US Department of Homeland Security (DHS)

- ***Cyber Safety Review Board (CSRB) -*** an independent public-private advisory body administered by DHS through CISA, brings together public and private sector cyber experts/leaders to review and draw lessons learned from the most significant cyber incidents
- ***Transportation Security Agency (TSA)*** - efforts include a combination of cybersecurity assessments and engagements; stakeholder education; publication of cybersecurity guidance and best practices; and use of its regulatory authority to mandate appropriate and durable cybersecurity measures
- ***United States Coast Guard (USCG)*** - combat cyber threats and protect U.S. maritime interests both domestically and abroad; continually promotes best practices, identifies potential cyber-related vulnerabilities, implements risk management strategies, and has in place key mechanisms for coordinating cyber incident responses
- ***United States Secret Service (USSS)*** investigates a range of cyber-enabled crime with a particular focus on protecting the nation's financial infrastructure
- ***Immigration and Customs Enforcement - Homeland Security Investigations (ICE HSI)*** - worldwide law enforcement leader in dark net and other cyber-related criminal investigations
- ***Office of the Chief Information Officer (OCIO)*** ensures strong cybersecurity practices within DHS, so that the Department may lead by example
- ***Office of Policy*** - leading the whole of federal government effort to coordinate, de-conflict, and harmonize cyber incident reporting requirements through the Cyber Incident Reporting Council

Cybersecurity in the US
US Government – Cybersecurity and Infrastructure Security Agency (CISA)

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

    Acts as the quarterback for the federal cybersecurity team, protecting and defending the home front—our federal civilian government networks—in close partnership with the Office of Management and Budget, which is responsible federal cyber security overall

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

    Look at the entire threat picture and work with partners across government and industry to defend against today's threats while securing the nation's critical infrastructure against threats that are just over the horizon

Cybersecurity Frameworks

Cybersecurity Frameworks

- Multiple cybersecurity frameworks exist
- Developed by both US Government agencies and industry associations
- Some important examples of cybersecurity frameworks in the US:
  - NIST Framework for Improving Critical Infrastructure Cybersecurity
  - Center for Internet Security Critical Security Controls
  - Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)
  - International Society of Automation ISA/IEC 62443
  - International Telecommunications Union (ITU) National Cybersecurity / Critical Information Infrastructure Protection (CIIP)
  - Internet of Things Security Foundation (IoTSF) Security Assurance Framework
  - ISO 27001 / ISO 27002
  - NIST SP 800-53R5

NIST Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1 issued April 16, 2018

Goal is 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

NIST Framework for Improving Critical Infrastructure Cybersecurity

NIST Cybersecurity Framework Components:

- Framework Core - a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.
  - Consists of five concurrent and continuous Functions—Identify, Protect, Detect, Respond, Recover
  - Identifies underlying key Categories and Subcategories – which are discrete outcomes – for each Function
- 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"): 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

NIST Framework for Improving Critical Infrastructure Cybersecurity

Framework Core Functions:

- **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

NIST Framework for Improving Critical Infrastructure Cybersecurity

Developed sector-specific guidance that provides sector stakeholders with the ability to:

- Understand and use the Framework to assess and improve their cyber resiliency;
- Assess their current- and target-cybersecurity posture;
- Identify gaps in their existing cybersecurity risk management programs, and;
- Identify current, sector-specific tools and resources that map to the Framework

Sector-specific guidance has been developed for the following critical sectors:

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

Center for Internet Security Critical Security Controls

Version 8 issued May 2021

Purpose is to:

- Share insights into attacks and attackers, identify root causes, and translate that into classes of defensive action
- Create and share tools, working aids, and stories of adoption and problem-solving
- Map the CIS Controls to regulatory and compliance frameworks to ensure alignment and bring collective priority and focus to them Identify common problems and barriers (like initial assessment and implementation roadmaps), and solve them as a community
- Reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals), with every role (threat responders and analysts, technologists, information technology (IT) operators and defenders, vulnerability-finders, tool makers, solution providers, users, policy-makers, auditors, etc.), and across many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT, etc.)

Center for Internet Security Critical Security Controls

Security Controls

- **Inventory and Control of Enterprise Assets:** Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments to support identifying unauthorized and unmanaged assets to remove or remediate
- **Inventory and Control of Software Assets:** Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution
- **Data Protection:** Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data
- **Secure Configuration of Enterprise Assets and Software:** Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications)
- **Account Management**: Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software
- **Access Control Management:** Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software

Center for Internet Security Critical Security Controls

Security Controls

- **Continuous Vulnerability Management:** Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, to remediate, and minimize, the window of opportunity for attackers and monitor public and private industry sources for new threat and vulnerability information
- **Audit Log Management:** Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack
- **Email and Web Browser Protection:** Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement
- **Malware Defenses:** Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets
- **Data Recovery**: Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state
- **Network Infrastructure Management**: Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points

Center for Internet Security Critical Security Controls

Security Controls

- **Network Monitoring and Defense**: Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base
- **Security Awareness and Skills Training:** Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise
- **Service Provider Management:** Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately
- **Application Software Security**: Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise
- **Incident Response Management**: Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack
- **Penetration Testing:** Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker

Cloud Security Alliance (CSA) Cloud Control Matrix (CCM)

- Cybersecurity control framework for cloud computing
- Composed of 197 control objectives that are structured in 17 domains covering all key aspects of cloud technology
- Used as a tool for the systematic assessment of a cloud implementation, and provides guidance on which security controls should be implemented by which actor within the cloud supply chain
- Is aligned to the CSA Security Guidance for Cloud Computing, and is considered a de-facto standard for cloud security assurance and compliance
- Includes the following:
  - CCM v4 Controls
  - Mappings
  - CAIQ v4
  - Implementation Guidelines
  - Auditing Guidelines
  - CCM Metrics

International Society of Automation ISA/IEC 62443

- An international series of standards that address cybersecurity for operational technology in automation and control systems
- improve the safety, availability, integrity and confidentiality of components or systems used for industrial automation and control, and to provide criteria for procuring and implementing secure industrial automation and control systems
- Directed towards those responsible for designing, implementing, or managing industrial automation and control systems
- Applies to users, system integrators, security practitioners, and control systems manufacturers and vendors
- Builds on established standards for the security of general purpose information technology systems (e.g., the ISO/IEC 27000 series)
- Identifies and addresses the important differences present in Industrial Automation and Control Systems (IACS)

International Society of Automation ISA/IEC 62443 - Organization

General – This group includes elements that address topics that are common to the entire series

- 62443-1-1 standard introduces the concepts and models used throughout the series.
- 62443-1-2 technical report contains a master glossary of terms and abbreviations used throughout the series
- 62443-1-3 standard describes a series of quantitative metrics derived from the foundational requirements, system requirements and associated
- 62443-1-4 technical report provides a more detailed description of the underlying life cycle for IACS security, as well as several use cases that illustrate various applications.

Policies and Procedures – Elements in this group focus on the policies and procedures associated with IACS security

- 62443-2-1 standard describes what is required to define and implement an effective IACS cyber security management system
- 62443-2-2 standard provides specific guidance on what is r equired to operate an effective IACS cyber security management system
- 62443-2-3 technical report provides guidance on the specific subject of patch management for IACS
- 62443-2-4 standard specifies requirements for suppliers of IACS

International Society of Automation ISA/IEC 62443 - Organization

System Requirements – Elements in the third group address requirements at the system level

- 62443-3-1 technical report describes the application of various security technologies to an IACS environment
- 62443-3-2 standard addresses security risk assessment and system design for IACS
- 62443-3-3 standard describes the foundational system security requirements and security assurance levels

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

- 62443-4-1 standard describes the derived requirements that are applicable to the development of products
- 62443-4-2 standard contains sets of derived requirements that provide a detailed mapping of the system requirements to subsystems and components of the system under consideration

International Telecommunictions Union (ITU) Critical Information Infrastructure Protection (CIIP)

Dated August 2007

- Help countries to determine their response to the challenges of CIIP
- Draws on different existing CIIP models, in particular, the Swiss CIIP model, to suggest a functional model for a CIIP unit that can promote collaboration between existing stakeholders to protect the state's critical infrastructure and services
- Four pillars of CIIP:
  - **Prevention and Early Warning** - Ensure that companies operating critical infrastructures are prepared to cope with incidents through activities that raise the general preparedness of companies
  - **Detection** – Ensure that new threats be discovered as quickly as possible
  - **Reaction** - Includes the identification and correction of the causes of a disruption
  - **Crisis Management** - Minimize the effects of any disruptions on society and the state

Internet of Things Security Foundation (IoTSF) Security Assurance Framework

Release 3.0 Dated November 2021

- A structured process of questioning and evidence gathering to ensure suitable security mechanisms and practices are implemented
- Is intended to help all companies make high-quality, informed security choices by guiding them through a comprehensive requirement checklist and evidence gathering process - the evidence gathered during the process can be used to declare conformance with best practice to customers and other stakeholders
- Can be used internally in an organization as a pre-compliance tool to self-assess or self-certify against, or by a third-party auditor
- Can also be used ‘in part’, as a procurement mechanism to help specify security requirements of a supplier contract

Internet of Things Security Foundation (IoTSF) Security Assurance Framework

Framework Stakeholders:

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

Framework Scope:

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

Internet of Things Security Foundation (IoTSF) Security Assurance Framework

Process Steps:

- **Risk Assessment** - Conduct Risk Analysis of product in target environment
- **Assurance Class** - Determine Assurance Class applicable to the product
- **Using the Assurance Questionnaire** - Respond to each question in the framework document

Framework includes separate questions for the following categories:

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

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

Version 2005-11 dated October 15, 2005

- Is an international standard for the implementation of an enterprise-wide Information Security Management System (ISMS)
- Covers all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations
- Specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks
- Specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof
- Ensures the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties
- ISO 27001 standard is required by:
  - Organizations carrying sensitive information, regardless of their size, be it public or private, IT or non-IT
  - Organizations expanding their business and seeking new clients
  - Contractors that need to be ISO 27001 compliant to score projects

ISO 27001 Information technology — Security techniques — Information security management systems — Requirements

ISO 27001 Domains:

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

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

Dated June 15, 2005

- Establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization
- Provides general guidance on the commonly accepted goals of information security management
- Control objectives and controls are intended to be implemented to meet the requirements identified by a risk assessment
- Main clauses are the same as the main categories in ISO/IEC 27001
- Each clause has one or more main security categories that provide information on:
  - Control objective
  - Controls that can be applied to achieve the control objective.
  - A specific control statement to satisfy the control objective.
  - Implementation guidance
  - Further information that may need to be considered

NIST SP 800-53R5 Security and Privacy Controls for Information Systems and Organizations

Dated September 2020

- Provides a catalog of security and privacy controls for information systems and organizations to protect organizational operations and assets, individuals, other organizations, and the Nation from a diverse set of threats and risks

Control Families

- Access Control
- Audit and Accountability
- Awareness and Training
- Configuration Management
- Contingency Planning
- Assessment
- Authorization and Monitoring
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical and Environmental Protection
- Planning
- Risk Assessment
- System and Services Acquisition
- System and Information Integrity
- Program Management
- PII Processing and Transparency
- Supply Chain Risk Management
- System and Communications Protection

HCD Security Guidelines

Liaison Status

Trusted Computing Group (TCG)

- **Next TCG Members Meetings**
  - **TCG Hybrid F2F (Vancouver, BC) – 21-23 February 2023 – Ira to call in**
  - **TCG Hybrid F2F (Munich, Germany) – TBD June 2023 – Ira to call in**
- **Trusted Mobility Solutions (TMS) – Ira is co-chair and co-editor**
  - **Formal Liaisons – GP (TEE, SE, TPS), ETSI (NFV/MEC/SAI Security and Privacy)**
  - **Informal Liaisons – 3GPP, GSMA, IETF, ISO, ITU-T, SAE, US NIST**
  - ***TCG TMS Use Cases v2 – published September 2018***
- **Mobile Platform (MPWG) – Ira is co-editor**
  - **Formal and Informal Liaisons – jointly with TMS WG above**
  - ***TCG Mobile Reference Architecture v2 – work-in-progress for review Q1/Q2 2023***
  - ***TCG TPM 2.0 Mobile Common Profile – work-in-progress for review Q1/Q2 2023***
  - ***TCG MARS 1.0 Mobile Profile – new work-in-progress Q4 2021***
  - ***TCG Runtime Integrity Preservation for Mobile Devices – published Nov 2019***
  - ***GP TPS Client API / Entity Attestation Protocol / COSE Keystore – joint work***
- **Recent Specifications**
  - **http://www.trustedcomputinggroup.org/resources**
  - ***TCG Measurement and Attestation RootS Library – published January 2023***
  - ***TCG Storage Opal Family Feature Set: C_PIN – public review January 2023***
  - ***TCG Storage Interface Interactions Spec (SIIS) – public review December 2022***
  - ***TCG DICE Endorsement Architecture for Devices – published November 2022***
  - ***TCG Component Class Registry – review October 2022***
  - ***TCG Storage Component Class Registry – review October 2022***

Internet Engineering Task Force (IETF) (1 of 4)

- **Next IETF Members Meetings**
  - **IETF 116 Hybrid F2F (Yokohama, Japan) – 27-31 March 2023 – Ira to call in**
  - **IETF 117 Hybrid F2F (San Francisco, CA) – 24-28 July 2023 – Ira to call in**
- **Transport Layer Security (TLS)**
  - **IETF Exported Authenticators in TLS – RFC 9261 – July 2022**
    https://datatracker.ietf.org/doc/rfc9261/
  - **IETF Importing External Pre-Shared Keys (PSKs) for TLS 1.3 – RFC 9258 – July 2022**
    https://datatracker.ietf.org/doc/rfc9258/
  - **IETF Guidance for External Pre-Shared Key (PSK) Usage in TLS – RFC 9257 – July 2022**
    https://datatracker.ietf.org/doc/rfc9257/
  - **IETF TLS Ticket Requests – RFC 9149 – April 2022**
    https://datatracker.ietf.org/doc/rfc9149/
  - **IETF DTLS Protocol Version 1.3 – RFC 9147 – April 2022**
    https://datatracker.ietf.org/doc/rfc9147/
  - **IETF IANA Registry Updates for TLS/DTLS – draft-03 – February 2023**
    https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8447bis/
  - **IETF Identity Module for TLS Version 1.3 – draft-08 – January 2023**
    https://datatracker.ietf.org/doc/draft-urien-tls-im/
  - **IETF Flags Extension for TLS 1.3 – draft-11 – January 2023**
    https://datatracker.ietf.org/doc/draft-ietf-tls-tlsflags/
  - **IETF Compact TLS 1.3 – draft-07-January 2023**
    https://datatracker.ietf.org/doc/draft-ietf-tls-ctls/
  - **IETF NULL Encryption & Key Exchange w/o Forward Secrecy Discouraged – draft-05 – January 2023**
    https://datatracker.ietf.org/doc/draft-mattsson-tls-psk-ke-dont-dont-dont/
  - **IETF Compact ECDHE and ECDSA Encodings for TLS 1.3 – draft-03 – January 2023**
    https://datatracker.ietf.org/doc/draft-mattsson-tls-compact-ecc/
  - **IETF Suppressing CA Certificates in TLS 1.3 – draft-03 – January 2023**
    https://datatracker.ietf.org/doc/draft-kampanakis-tls-scas-latest/
  - **IETF Deprecating Obsolete Key Exchange Methods in TLS – draft-01 – December 2023**
    https://datatracker.ietf.org/doc/draft-ietf-tls-deprecate-obsolete-kex/

Internet Engineering Task Force (IETF) (2 of 4)

- **Security Automation and Continuous Monitoring (SACM)**
  - **IETF SACM WG – closed July 2022 – IETF Security ADs**
    https://mailarchive.ietf.org/arch/msg/sacm/3UYKoLiQWA2h6CbIxBbCXGG6Qi4/
  - **IETF Concise Software Identifiers – draft-22 – Sept 2022 – RFC Editor**
    https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/
- **Concise Binary Object Representation (CBOR)**
  - **IETF Stable Storage for Items in CBOR – RFC 9277 – August 2022**
    https://datatracker.ietf.org/doc/rfc9277/
  - **IETF Additional Control Ops for CDDL – RFC 9165 – December 2021**
    https://datatracker.ietf.org/doc/rfc9165/
  - **IETF CBOR tags for IPv4/v6 Adresses – RFC 9164 – December 2021**
    https://datatracker.ietf.org/doc/rfc9164/
  - **IETF CBOR Tags for OIDs – RFC 9090 – July 2021**
    https://datatracker.ietf.org/doc/rfc9090/
  - **IETF Packed CBOR – draft-08 – January 2023**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-packed/
  - **IETF CBOR Tags for Time, Duration, and Period – draft-04 – January 2023**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-time-tag/
  - **IETF Feature Freezer for CDDL – draft-10 – October 2022**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-freezer/
  - **IETF App-Oriented Literals in CBOR Ext Diag Notation – draft-01 – October 2022**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-edn-literals/
  - **IETF CDDL 2.0 -- a draft plan - draft-00 - October 2022**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-2-draft/
  - **IETF Using CDDL for CSVs – draft-01 – August 2022**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-csv/
  - **IETF Notable CBOR Tags – draft-07 – July 2022**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-notable-tags/

Internet Engineering Task Force (IETF) (3 of 4)

- **Remote ATtestation ProcedureS (RATS)**
  - **IETF RATS Architecture – RFC 9334 – January 2023**
    https://datatracker.ietf.org/doc/rfc9334/
  - **IETF CBOR Tag for Unprotected CWT Claims Sets – draft-05 – February 2023**
    https://datatracker.ietf.org/doc/draft-ietf-rats-uccs/
  - **IETF Entity Attestation Token (EAT) – draft-19 – December 2022 – to IETF Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat/
  - **IETF EAT Collection Type – draft-02 – December 2022**
    https://datatracker.ietf.org/doc/draft-frost-rats-eat-collection/
  - **IETF Concise TA Stores (CoTS) – draft-00 – December 2022 – WG adopted**
    https://datatracker.ietf.org/doc/draft-ietf-rats-concise-ta-stores/
  - **IETF EAT-based Key Attestation Token - draft-00 - October 2022**
    https://datatracker.ietf.org/doc/draft-bft-rats-kat/
  - **IETF RATS Conceptual Messages Wrapper – draft-01 – October 2022**
    https://datatracker.ietf.org/doc/draft-ftbs-rats-msg-wrap/
  - **IETF Epoch Markers – draft-02 – October 2022**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-epoch-markers/
  - **IETF EAT-based Key Attestation Token – draft-00 – October 2022**
    https://datatracker.ietf.org/doc/draft-bft-rats-kat/
  - **IETF EAT Media Types – draft-01 – October 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat-media-type/
  - **IETF Direct Anonymous Attestation for RATS – draft-02 – September 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-daa/
  - **IETF Attestation Event Stream Subscription - draft-02 - September 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-network-device-subscription/
  - **IETF Reference Interaction Models for RATS - draft-06 - September 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/
  - **IETF Attestation Results for Secure Interactions - draft-03 - September 2022**
    https://datatracker.ietf.org/doc/draft-ietf-rats-ar4si/

Internet Engineering Task Force (IETF) (4 of 4)

- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **IRTF Hybrid Public Key Encryption – RFC 9180 – February 2022**
    https://datatracker.ietf.org/doc/rfc9180/
  - **IRTF Argon2 password hash and proof-of-work – RFC 9106 – September 2021**
    https://datatracker.ietf.org/doc/rfc9106/
  - **IRTF Oblivious PRFs w/ Prime-Order Groups – draft-20 – February 2023 – to IRSG**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/
  - **IRTF RSA Blind Signatures - draft-09 - February 2023 – to IRTF Chair**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-rsa-blind-signatures/
  - **IRTF Key Blinding for Signature Schemes – draft-03 – January 2023**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-signature-key-blinding/
  - **IRTF Usage Limits on AEAD Algorithms – draft-06 – January 2023**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-limits/
  - **IRTF AEGIS family of authenticated encryption algorithms – draft-01 – January 2023**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aegis-aead/
  - **IRTF Two-Round Threshold Schnorr Sigs with FROST – draft-12 – January 2023 – to RG LC**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-frost/
  - **IRTF CPace, a balanced composable PAKE – draft-07 – January 2023**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-cpace/
  - **IRTF Properties of AEAD algorithms - draft-00 – December 2022 – WG adopted**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-properties/
  - **IRTF Deterministic Nonce-less HPKE – draft-00 – December 2022 – WG adopted**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-dnhpke/
  - **IRTF Ristretto255 and Decaf448 Groups - draft-05 - November 2022**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-ristretto255-decaf448/
  - **IRTF Combiner for Hybrid Key Encapsulation Mechanisms – draft-00 – November 2022**
    https://datatracker.ietf.org/doc/draft-ounsworth-cfrg-kem-combiners/

Next Steps – IDS WG

- Next IDS WG Meeting– February 23, 2023
- Next IDS Face-to-Face Meeting likely May 18, 2023 at PWG May 2023 F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG