The Printer Working Group

Imaging Device Security

August 19, 2020

PWG August 2020 Virtual Face-to-Face

Agenda

When	What
10:00 – 10:05	Introductions, Agenda review
10:05 – 10:45	Discuss results of latest HCD iTC Meetings and potential HCD cPP v1.0 content
10:45 – 11:10	Review of new ETSI IoT Security Standard
11:10 – 11:35	HCD Security Guidelines 1.0 Status
11:35 – 11:55	Status of other HCD Security Standards Efforts
11:55 – 12:00	Wrap Up / Next Steps

Intellectual Property Policy

“This meeting is conducted under the rules of the PWG IP policy”.

- Refer to the IP statements in the plenary slides

Officers

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

HCD international Technical Community (iTC) Status

HCD international Technical Community (iTC)

- HCD iTC formally approved by Common Criteria Management Committee in Feb 2020

- Key HCD iTC Officers:
  - Chairperson – Kwangwoo Lee, HP
  - Deputy Chairperson – Alan Sukert
  - CCDB Liaison - Eunkyoung Yi, Korean Scheme
  - Editors – Alan Sukert; Brian Volkoff, Ricoh; Geraldo Colunga, HP
  - Record Manager – TBD (Kwangwoo Lee acting for now)

HCD international Technical Community (iTC)

- Agreed to hold bi-weekly meetings. Since last IDS F2F in May, meetings have been held on:
  - 5/28/2020
  - 6/11/2020
  - 6/25/2020
  - 7/9/2020
  - 7/23/2020
  - 8/6/2020
- Also held Editor’s Meetings on the off-weeks between the bi-weekly HCD iTC meetings

HCD iTC Status

Key Status:

- First internal draft of the HCD collaborative Protection Profile (cPP) released for HCD iTC review on 7/21; comments due by August 17th
  - Contains all the SFRs from HCD PP v1.0 and v1.1
- First internal draft of the HCD Supporting Document (SD) should be released for HCD iTC review on 8/17
  - Contains all the Assurance Activities from HCD PP
- Both internal drafts are to contain the contents of what would have been HCD PP v1.1, which should include:
  - HCD PP v1.0 as approved by NIAP and JISEC
  - HCD PP Errata #1
  - All NIAP Technical Decisions against the HCD PP
  - All changes to HCD PP v1.0 approved by the HCD Technical Committee before it became the HCD iTC

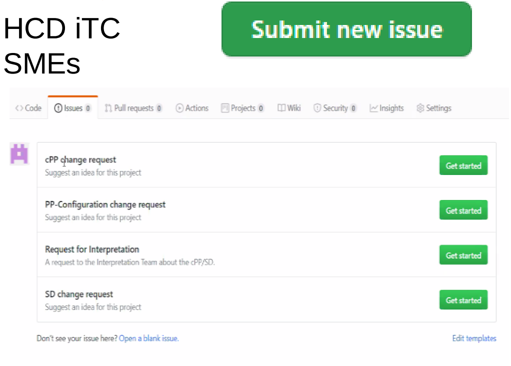
HCD-iTC-Admin-template/Review_Process.adoc

HCD iTC will publish the draft cPP (file format : .pdf) w/o page number

Update the PR Status

Editors

HCD iTC SMEs



Submit new issue

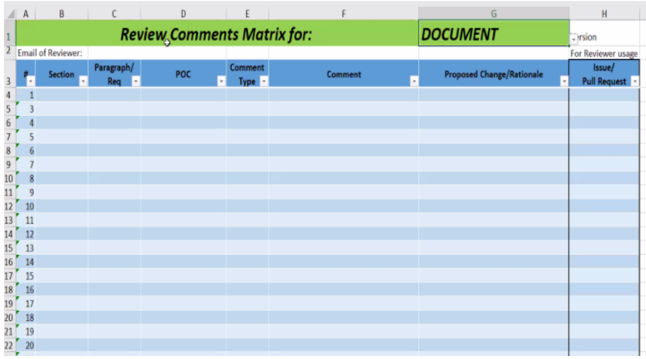
cPP change request
Suggest an idea for this project
Get started

PP-Configuration change request
Suggest an idea for this project
Get started

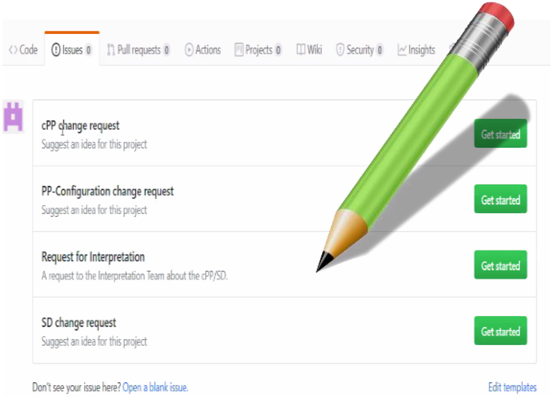
Request for Interpretation
A request to the Interpretation Team about the cPP/SD.
Get started

SD change request
Suggest an idea for this project
Get started

Don't see your issue here? Open a blank issue.
Edit templates



	A	B	C	D	E	F	G	H
1	Review Comments Matrix for:						DOCUMENT	rsion
2	Email of Reviewer:							For Reviewer usage
3	#	Section	Paragraph/ Req	POC	Comment Type	Comment	Proposed Change/Rationale	Issue/ Pull Request
4	1							
5	3							
6	4							
7	5							
8	6							
9	7							
10	8							
11	9							
12	10							
13	11							
14	12							
15	13							
16	14							
17	15							
18	16							
19	17							
20	18							
21	19							
22	20							



cPP change request
Suggest an idea for this project
Get started

PP-Configuration change request
Suggest an idea for this project
Get started

Request for Interpretation
A request to the Interpretation Team about the cPP/SD.
Get started

SD change request
Suggest an idea for this project
Get started

Don't see your issue here? Open a blank issue.
Edit templates

Submit Review comment
- Github "New issue"

Create the Master spreadsheet
(Review Comments Matrix)

cPP (Alan)
SD (Jerry)

Implementation
cPP (Brian)
SD (Jerry)

Sanity Check

Chair

Triage
(Editorial, General, Technical)
Review the proposal
Decision Making - Vote

HCD iTC Editors meeting
□ HCD iTC biweekly meeting

EAL Claim for HCD cPP

- **Option 1 : No EAL Claim (SARs of EAL2 without ALC_FLR)**
  - Pro
    - Reduces the risk for requiring vendors to double-certify (which is the current situation for some vendors).
  - Cons :
    - Longer timeline for developing the cPP/SD due to the additional work needed to implement EAs for SARs of EAL2.
    - Longer timeline for evaluations due to the additional SARs which require a vendor to generate additional evaluation evidence (e.g. TOE Design, Delivery, etc.).
    - Risk for NIAP to not endorse the cPP/SD.
- **Option 4 : No EAL Claim (SARs of EAL1 without ALC_FLR)**
  - Pros
    - Shorter timeline for developing cPP/SD.
    - Shorter timeline for evaluations.
    - Lower risk for NIAP not to endorse the cPP/SD.
  - Con
    - Higher risk for requiring vendors to double-certify

EAL Claim for HCD cPP

- Could not achieve consensus so it was agreed to put it to a vote of the entire HCD iTC
- Voting Rules: Vote is for either
  - **Option 1 : No EAL Claim (SARs of EAL2 without ALC_FLR)**
  - **Option 4 : No EAL Claim (SARs of EAL1 without ALC_FLR)**

  Voting Rules
  - One vote is allowed for each member organization, not for each individual member.
  - “Organization” is defined according to the definition adopted by the CC Users Forum; for commercial enterprises, a parent company and all of its divisions and subsidiaries constitute one organization.
  - Votes submitted shall be explicit: **Option 1**, **Option 4**.
  - At the end of the voting period, ballots are tabulated and reviewed by the Chair or the Technical Editor. Results of voting are posted, including a summary of the vote and the votes cast by each organization.
  - An approval criteria will be simple majority for this voting.

EAL Claim for HCD cPP

Results

Candidate	Total Votes
Option 1	7
Option 4	15
Total Votes	22

There were 22 votes cast in all, by a total of 22 of different entities.
7 entities votes for a option 1, while 15 entities votes for a option 4
If anyone has any questions relating to the results then please feel free to ask.

Total Organizations in HCD iTC	31

HCD iTC Status
Proposed Public Review Process for HCD cPP Documentation

Phase	Timeline	Description
Internal Draft	1st working draft release : 2020.07.21 (Tue) * Call for comment (SME) : 2020.07.21 (Wed) ~ 2020.08.17 (Mon) [4W] * Comment resolution : 2020.08.18 (Tue) ~ 2020.09.22 (Tue) [5W] * Editors works : 2020.09.23 (Wed))- 2020.10.19(Mon) [4W] 2nd working draft release : 2020.10.20 (Tue) * Call for comment : 2020.10.20 (Tue) ~ 2020.11.16 (Mon) [4W] * Comment resolution : 2020.11.17 (Tue) - 2020.12.18 (Fri) [4.5W] * Editors works : 2020.12.19 (Sat) – 2021.2.1 (Mon) [5.5W] (Editor's time off : End of 2020)	The normal, pre-release process for creating the working draft. 1st WD : Initial version - 2020.07.21 - *File name: HCD-CPP DRAFT 07-21-2020.pdf* 2nd WD : Ed, Ge, Te, New work item (at least title) – Date - *File name: HCD-CPP DRAFT 10-20-2020.pdf* Public Review Draft 1 : Ed, Ge, Te (**V0.6X**) Public Review Draft 2 : Ed, (Ge, Te) (**V0.7X**) [Optional] Public Review Draft 3 : Ed (**V0.8X**) Proposed Draft : Ed (**V0.9X**) Final Document Published (**V1.0**)
Public Review Draft 1	45 days (2021.02.02 (Tue) ~ 2021.03.19 (Fri)	HCD-iTC has voted according to Terms of Reference to release this version for public review. Public (i.e. from non-iTC participants) comments are accepted during this period
Public Review Draft 1 Update	Up to 60 days (2021.03.20 (Sat) ~ 2021.05.17 (Mon))	The HCD-iTC will review all received comments and update the documents accordingly
Public Review Draft 2	45 days (2021.05.18 (Tue) ~ 2021.07.01 (Thu))	HCD-iTC has voted according to Terms of Reference to release this version for public review. Public (i.e. from non-iTC participants) comments are accepted during this period
Public Review Draft 2 Update	Up to 60 days (2021.07.02 (Fri) ~ 2021.08.28(Sat))	The HCD-iTC will review all received comments and update the documents accordingly
Proposed Draft	30 days+ (2021.08.29 (Sun) ~ 2021.09.30(Thu))	HCD-iTC has voted according to Terms of Reference to propose this as the final document. Public (i.e. from non-iTC participants) comments are accepted during this period
Proposed Update	10 days+ (2021.10.01(Fri) ~ 2021.10.12 (Tue)	HCD-iTC reviews any further comments and prepares the document for final publishing (updating all dates, producing official versions for publication)
Final Document Published		Documents are posted to Common Criteria Portal

HCD iTC Status
Other Issues

- Inclusion of ALC_FLR
  - Problem will be developing assurance activities for ALC_FLR that will meet NIAP’s requirements of being “achievable”, “repeatable”, “testable” & “consistent”
- When to start adding new SFRs and Assurance Activities into the HCD cPP and SD drafts
  - Should be ASAP
- What new SFRs and Assurance Activities should we include in HCD cPP/SD v1.0:
  - Split TLS (and maybe SSH) requirements into separate server and client requirements (a must have)
    - Problem is which version of the split requirements to use – are different TLS packages and the version in ND cPP v2.2e
  - Reflect any new NIAP/JISEC Technical Decisions (a must have)

HCD iTC Status
Other Issues

- What new SFRs and Assurance Activities should we include in HCD cPP/SD v1.0 (cont'd):
  - Support for FIPS 140-3 (a must have)
  - Removal of all SHA-1 support (a must have)
  - Removal of support for TLS 1.0 and TLS 1.1 (a must have)
  - Support for TLS 1.3 (If requirements are included in ND cPP/SD in time)
  - Anything that the HCD iTC as a group determines over the next 6-9 months is an "absolute must have" in v1.0; anything less has to go in v1.1 or later. Possible candidates include:
    - Expansion of network-fax separation to "no bridging"
    - Syncing with ENISA and the new proposed European cybersecurity certification scheme (EUCC)
    - Syncing with applicable updates to ND cPP and FDE cPPs
    - Syncing with any applicable NIST SP updates

ETSI EN 303 645 V2.1.1 (2020-06)
Cyber Security for Consumer Internet of Things

ETSI EN 303 645 V2.1.1 (2020-06)
Cyber Security for Consumer Internet of Things

Scope

Consumer IoT devices that are connected to network infrastructure (such as the Internet or home network)

Note: The standard defines a consumer IoT device as a “network-connected (and network-connectable) device that has relationships to associated services and are used by the consumer typically in the home or as electronic wearables”

Examples given in the standard would suggest the standard only applies to what we would typically consider consumer products – toys, TVs, smart phones, computers, home appliances, etc. However, the definition of consumer IoT device in this standard could be interpreted to apply to a home printer or desktop MFP purchased strictly for home use, so this standard could apply to HCDs.

ETSI EN 303 645 V2.1.1 (2020-06)
Cyber Security for Consumer Internet of Things

Requirements Categories:

- Passwords
  - Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user
  - Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage
  - Constrained Device - device which has physical limitations in either the ability to process data, the ability to communicate data, the ability to store data or the ability to interact with the user, due to restrictions that arise from its intended use

ETSI EN 303 645 V2.1.1 (2020-06)
Cyber Security for Consumer Internet of Things

Requirements Categories:

- Vulnerability Management
  - The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum:
    - initial acknowledgement of contact information for the reporting of issues; and
    - information on timelines for:
      - receipt; and
      - status updates until the resolution of the reported issues.
- Software Update
  - Many Software Update requirements (more than any other category)
  - Automatic mechanisms should be used for software updates.
  - The device should check after initialization, and then periodically, whether security updates are available.
  - The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update
  - The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period

ETSI EN 303 645 V2.1.1 (2020-06)
Cyber Security for Consumer Internet of Things

Requirements Categories:

- Secure Parameter Storage
  - Sensitive security parameters in persistent storage shall be stored securely by the device
  - Hard-coded critical security parameters in device software source code shall not be used
- Secure Communication
  - The consumer IoT device shall use best practice cryptography to communicate securely
  - Cryptographic algorithms and primitives should be updateable ("cryptoagility")
  - Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage

ETSI EN 303 645 V2.1.1 (2020-06)
Cyber Security for Consumer Internet of Things

Requirements Categories:

- Minimize Attack Surface
  - All unused network and logical interfaces shall be disabled
  - In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information
  - Device hardware should not unnecessarily expose physical interfaces to attack
- Software Integrity
  - The consumer IoT device should verify its software using secure boot mechanisms
  - If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function

ETSI EN 303 645 V2.1.1 (2020-06) **Cyber Security for Consumer Internet of Things**

Requirements Categories:

- Securing Personal Data
  - The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography
  - The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage
- System Resiliency
  - Resilience should be built in to consumer IoT devices and services, taking into account the possibility of outages of data networks and power
  - Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power

ETSI EN 303 645 V2.1.1 (2020-06)
Cyber Security for Consumer Internet of Things

Requirements Categories:

- System Telemetry Data
  - If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies
- Data Deletion
  - The user shall be provided with functionality such that user data can be erased from the device in a simple manner
  - Users should be given clear instructions on how to delete their personal data
- Installation and Maintenance
  - Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability
  - The manufacturer should provide users with guidance on how to securely set up their device
  - The manufacturer should provide users with guidance on how to check whether their device is securely set up

ETSI EN 303 645 V2.1.1 (2020-06)
Cyber Security for Consumer Internet of Things

Requirements Categories:

- Input Data Validation
  - The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices
- Data Protection
  - The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers
  - If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes

Some Ideas on Enforcement of the Standard*

- The new EN 303 645 standard set by ETSI doesn’t necessarily indicate enforcement, it paves the way for certifications that help towards that under various other regulatory enforcement. For example, ENISA, under its EU cybersecurity Act, is likely to pick up the EN 303 645 standard and then enforce it.
- In another scenario, where there is a security breach in an internet-connected device which involves a data compromise under GDPR regulations. “If as a manufacturer you can say you followed every recommendation in the EN, the data commissioner may look on your case more favorably. But if you simply said you thought about it but did nothing about following the recommendations, then there is no case to answer and there could be significant financial penalties under GDPR rules.”

*From EE Times Europe, July 3, 2020

ETSI EN 303 645 V2.1.1 (2020-06)
Cyber Security for Consumer Internet of Things

Some Ideas on Enforcement of the Standard*

- On another dimension, the new standard also helps with consumer confidence in the security of everyday products that connect to the internet. You could then have a scheme which certifies products under a traffic light system – green means it meets the standard. For consumers who are unlikely to understand the technicalities of their connected wearables or connected products, this will help in identifying which products they can buy with assurance that it meets some cybersecurity standards

*From EE Times Europe, July 3, 2020

Note: ETSI is also developing a test specification and an implementation guide to complement this standard which may provide additional guidance on enforcement of the standard; no dates for completion of these documents have been provided

HCD Security Guidelines Status

Other HCD Security Standards Activities

Potential Standards Activities To Be Watched

(3) US NIST - FREE!

* LWC (Lightweight Cryptography)

-- https://www.nist.gov/programs-projects/lightweight-cryptography

-- for resource-constrained devices (including mobile phones)

* TC (Threshold Cryptography)

-- https://csrc.nist.gov/Projects/Threshold-Cryptography

-- multi-party signatures and encryption algorithms - hot stuff!

* CF (Cybersecurity Framework)

-- https://www.nist.gov/cyberframework

* PQC (Post-Quantum Crypto)

-- https://csrc.nist.gov/Projects/Post-Quantum-Cryptography

* SWID (Software Identification Tags)

-- https://csrc.nist.gov/Projects/Software-Identification-SWID

-- see also https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/

-- underlies runtime integrity and remote attestation work

* SWA (Software Assurance)

-- https://www.nist.gov/itl/ssd/software-assurance

NIST CYBERSECURITY FRAMEWORK

NIST CyberSecurity Framework

- Risk-based approach to managing cybersecurity risk
- Composed of three parts:
  - Framework Core -- Set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors
    - Desired cybersecurity outcomes organized in a hierarchy and aligned to more detailed guidance and controls
  - Framework Implementation Tiers -- Provide context on how an organization views cybersecurity risk and the processes in place to manage that risk
    - Alignment of an organization’s requirements and objectives, risk appetite and resources ***using*** the desired outcomes of the Framework Core
  - Framework Profiles -- Represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories
    - A qualitative measure of organizational cybersecurity risk management practices

NIST CyberSecurity Framework Framework Core Elements

- **Functions**: Organize basic cybersecurity activities at their highest level
  - Functions are Identify, Protect, Detect, Respond, and Recover
- **Categories**: Subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.
  - Examples of Categories include “Asset Management,” “Identity Management and Access Control,” and “Detection Processes.”
- **Subcategories:** Further divide a Category into specific outcomes of technical and/or management activities.
  - Provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category
- **Informative References:** Specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory

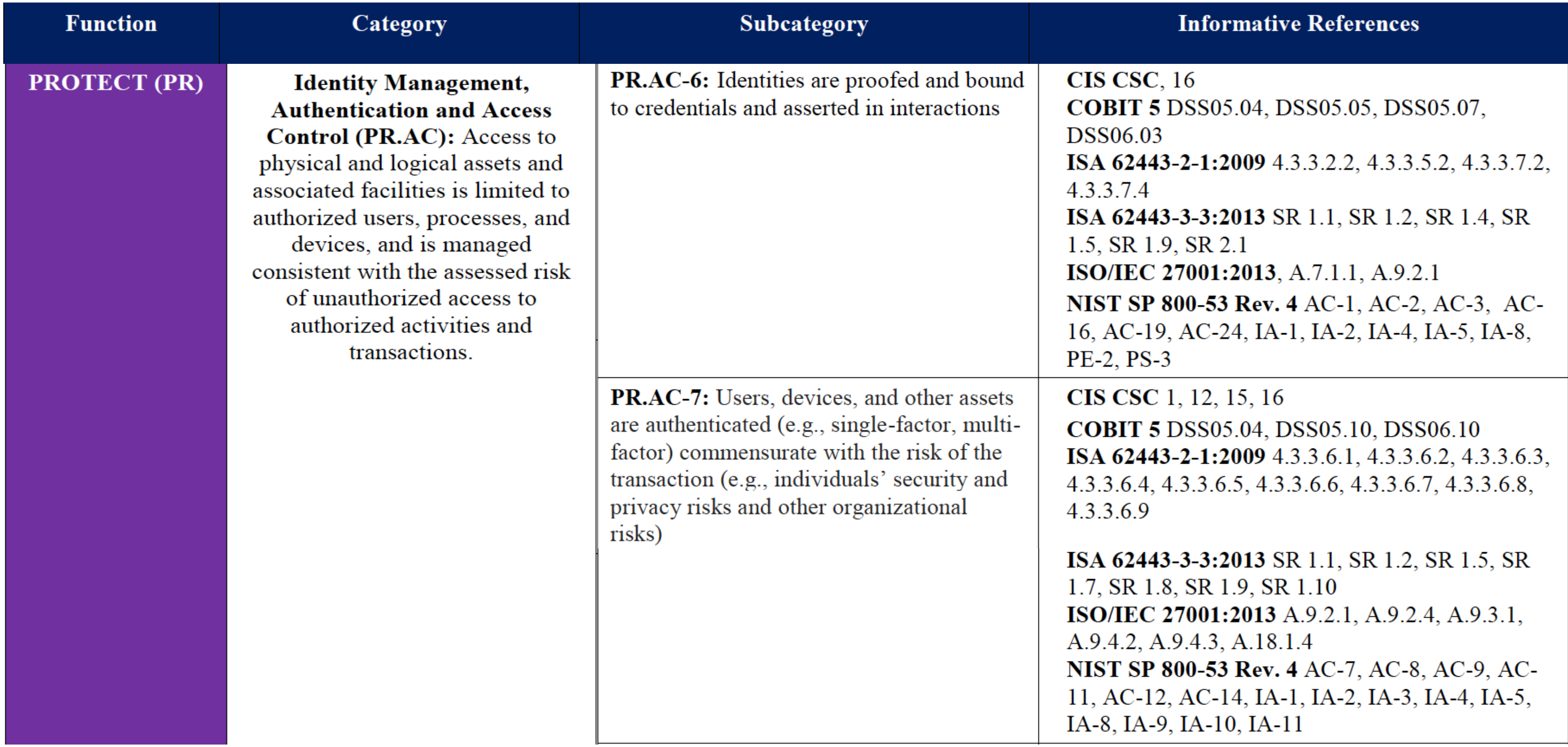
NIST CyberSecurity Framework
Framework Core

Function	
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 CyberSecurity Framework Functions and Categories

Function	Category
Identity	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Response	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

NIST CyberSecurity Framework Framework Core Excerpt



Function	Category	Subcategory	Informative References
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** 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.	**PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions	**CIS CSC**, 16 **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: 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)	**CIS CSC** 1, 12, 15, 16 **COBIT 5** DSS05.04, DSS05.10, DSS06.10 **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11

5 Functions 23 Categories 108 Subcategories 6 Informative References

NIST CyberSecurity Framework Implementation Tiers

	Risk Management Process	**Integrated Risk Management Program**	**External Participation**
Tier 1 Partial	• Ad hoc • Not formalized • Reactive	• Limited risk awareness • Implementation uneven	• No collaboration with other entities
Tier 2 Risk Informed	• Risks prioritized by needs • No organizational policy	• No organizational-wide approach or implementation	• Is some collaboration with others, but doesn’t always act on info
Tier 3 Repeatable	• Formal policy • Practices updated as needed	• Organization-wide approach • Processes/practices in place	• Regularly collaborates & shares info with other entities
Tier 4 Adaptive	• Adapts practices based on lessons learned, changing threats	• Becomes part of organizational culture	• Regularly uses and shares risk info with external entities

References

- NIST CyberSecurity Framework: https://www.nist.gov/cyberframework
- Link to ENISA Cybersecurity Standards and Certification page (w/ ENISA regulations); https://www.enisa.europa.eu/topics/standards
- IETF RFC on Constrained Devices Terminology: https://tools.ietf.org/html/rfc7228
- Excellent Wikipedia page on Crypto Agility: https://en.wikipedia.org/wiki/Crypto-agility#Best_practices
- IETF Guidelines on Crypto Agility: https://tools.ietf.org/html/rfc7696

Next Steps – IDS WG

- Next IDS Conference Call – Sep 3, 2020
- Next IDS Face-to-Face Meeting Nov 10-12 (probably Nov 12), 2020 at next Virtual PWG F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG

BACKUP

Trusted Computing Group (TCG)

- **Next TCG Members Meetings**
  - **TCG Virtual F2F – 12-16 October 2020 –Ira to call in**
  - **TCG Virtual F2F – TBD dates February 2021 –Ira to call in**
- **Trusted Mobility Solutions (TMS) – Ira is co-chair and co-editor**
  - **Formal – GP (TEE, SE), ETSI (NFV/MEC), ATIS (5G Security)**
  - **Informal – 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 – GP (TEE, SE), ETSI (NFV/MEC), ATIS (5G Security)**
  - ***TCG Runtime Integrity Preservation for Mobile Devices – Nov 2019***
  - ***TCG Mobile Reference Architecture v2 – work-in-progress***
  - ***TCG TPM 2.0 Mobile Common Profile – work-in-progress***
- **Recent Specifications**
  - **http://www.trustedcomputinggroup.org/resources**
  - ***TCG Algorithm Registry r1.32 – June 2020***
  - ***TCG TSS 2.0 Feature API (FAPI) – June 2020***
  - ***TCG TSS 2.0 Enhanced System Level API (ESAPI) – May 2020***
  - ***TCG TPM 2.0 Library r1.62 – review May 2020 – not for publication***
  - ***TCG TPM 2.0 Library r1.59 – March 2020***

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

- **Next IETF Members Meetings**
  - **IETF 109 Virtual F2F – 16-20 November 2020 – Ira to call in**
  - **IETF 110 Virtual F2F – 8-12 March 2021 – Ira to call in**
- **Transport Layer Security (TLS)**
  - **TLS 1.3 Extension Cert-Based Auth w/ Ext PSK – RFC 8773 – March 2020**
    https://tools.ietf.org/html/rfc8773
  - **Applying GREASE to TLS Extensibility – RFC 8701 – January 2020**
    https://tools.ietf.org/html/rfc8701
  - **TLS/1.3 – RFC 8446 – August 2018**
    https://tools.ietf.org/html/rfc8446
  - **Flags Extension for TLS 1.3 – July 2020**
    https://datatracker.ietf.org/doc/draft-ietf-tls-tlsflags/
  - **Delegated Credentials for TLS – June 2020**
    https://datatracker.ietf.org/doc/draft-ietf-tls-subcerts/
  - **Exported Authenticators in TLS – June 2020 – to IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-tls-exported-authenticator/
  - **Guidance for External PSK Usage in TLS – June 2020**
    https://datatracker.ietf.org/doc/draft-ietf-tls-external-psk-guidance/
  - **DTLS/1.3 – draft-38 – May 2020 – IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-tls-dtls14/
  - **Deprecating MD5 and SHA-1 in TLS 1.2 – May 2020 – to IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-tls-md5-sha1-deprecate/
  - **TLS Certificate Compression – draft-10 – January 2020 – RFC Editor**
    https://datatracker.ietf.org/doc/draft-ietf-tls-certificate-compression.txt

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

- **Security Automation and Continuous Monitoring (SACM)**
  - **Concise Software Identifiers – draft-15 – May 2020 – to IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/
  - **SACM Architecture – draft-06 – May 2020**
    https://datatracker.ietf.org/doc/draft-ietf-sacm-arch/
  - **Endpoint Posture Collection Profile – draft-01 – February 2020 – to IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-sacm-epcp/
- **Concise Binary Object Representation (CBOR)**
  - **CBOR Tags for Typed Arrays – RFC 8746 – February 2020**
    https://tools.ietf.org/html/rfc8746
  - **CBOR Sequences – RFC 8742 – February 2020**
    https://tools.ietf.org/html/rfc8742
  - **Concise Data Definition Language (CDDL) – RFC 8610 – June 2019**
    https://tools.ietf.org/html/rfc8610 - JSON/CBOR schema
  - **CBOR Tags for Date – draft-05 – July 2020 – to IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-date-tag/
  - **CBOR) Tags for OIDs – draft-00 – July 2020**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-tags-oid/
  - **CBORbis – draft-14 – June 2020 – to IETF LC**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-7049bis/

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

- **Remote ATtestation ProcedureS (RATS)**
  - **RATS Architecture – draft-05 – July 2020**
    https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/
  - **TPM-based Network Device RIV – draft-02 – July 2020**
    https://datatracker.ietf.org/doc/draft-ietf-rats-tpm-based-network-device-attest/
  - **Time-Based Uni-Directional Attestation – draft-03 – July 2020**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-tuda/
  - **Reference Interaction Models for RATS – draft-03 – July 2020**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-reference-interaction-model/
  - **YANG Data Model for CHARRA using TPMs – draft-02 – June 2020**
    https://datatracker.ietf.org/doc/draft-ietf-rats-yang-tpm-charra/
  - **CBOR Tag for Unprotected CWT Claims Sets – draft-01 – June 2020**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-uccs/
  - **Trusted Path Routing – draft-00 – June 2020**
    https://datatracker.ietf.org/doc/draft-voit-rats-trustworthy-path-routing/
  - **MUD-Based RATS Resources Discovery – draft-00 – March 2020**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-mud/
  - **Entity Attestation Token (EAT) – draft-03 – February 2020**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat/

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

- **IRTF Crypto Forum Research Group (CFRG) – future algorithms**
  - **Hybrid Public Key Encryption – draft-05 – July 2020 – RG LC**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hpke/
  - **Oblivious Pseudorandom Functions (OPRFs) – draft-04 – July 2020**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/
  - **Cpace Balanced Composable PAKE – draft-00 – July 2020**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-cpace/
  - **OPAQUE Asymmetric PAKE Protocol – draft-06 – June 2020**
    https://datatracker.ietf.org/doc/draft-krawczyk-cfrg-opaque/
  - **Hashing to Elliptic Curves – draft-09 – June 2020**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/
  - **Randomness for Security Protocols – draft-13 – June 2020**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-randomness-improvements/
  - **Pairing-Friendly Curves – draft-07 – June 2020**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves/
  - **Transition from Classical to Post-Quantum Cryptography – draft-07 – May 2020**
    https://datatracker.ietf.org/doc/draft-hoffman-c2pq/