The Printer Working Group

Imaging Device Security

May 18, 2023

PWG May 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, HIT and plans for future HCD cPP/HCD SD releases
10:45 – 11:25	US Cybersecurity Strategy / Plans
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 February 9, 2023 HCD iTC meetings have been held on:
  - February 13th
  - March 13th
  - April 10th
  - May 8th

  NOTE: Since publishing the HCD cPP v1.0 and HCD SD v1.0 in Oct 2022 the HCD iTC has gone to meeting once a month
- Current focus is on:
  - Developing a release plan for future versions of the HCD cPP and HCD SD
  - Determining content for and then implementing the next HCD cPP / HCD SD release
  - Addressing issues against HCD cPP / SD v1.0

HCD cPP/SD v1.0 Status

- Version 1.0 of both documents published on October 31, 2022
- Awaiting Endorsements from NIAP (US), ITSCC (Korea), JISEC (Japan)
  - NIAP is currently reviewing the HCD cPP (see HIT Slide)
  - As of TBD had no status on ITSCC or JISEC
- Canadian Scheme issued an Endorsement in Feb 2023
  - A vendor (Lexmark) is actively pursuing certification of an HCD against HCD cPP / HCD SD v1.0
- Created a list of the major changes between the current approved HCD PP (2015) and the newly published HCD cPP / SD v1.0 (2022)
  - 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, Evaluation Labs and NSA (representing NIAP)
  - Goal is to have the desired maximum of 10 members on the HIT
- HIT procedures v1.0 finalized and infrastructure set up
  - Using 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
  - Created new HCD-IT repository and Integration baseline for changes approved by the HIT
- Had first two HIT Meetings to review and process issues submitted for RfIs and approve HIT procedures v1.0 – See next 4 Slides

HCD cPP/SD HIT RfI Status

Issue #	Title	Issue	Status
HCD-IT #1	The FCS_COP.1/KeyEnc Cryptographic operation (Key Encryption) SFR in HCD cPP v1.0 is inconsistent with TPM 2.0 Architecture specification section 26.6 “Sensitive Area Encryption"	FCS_COP.1/KeyEnc SFR - Case: AES algorithm • AES used in [[selection: CBC, GCM] mode] TPM 2.0 Architecture specification Section 26.6 (Page 172) - "All symmetric encryption of the sensitive area uses Cipher Feedback (CFB) mode." CFB is the only AES mode allowed by the TPM 2.0 specification	Under Review – Looking at alternatives approach of using FPT_KYP_EXT.1.1 Key Protection SFR option where key is protected by another key that is not part of the key chain and update APP Notes to clarify options
HCD-IT #2	Clarification is needed about algorithm verification of Root of Trust in the Test Assurance activities for the Secure Boot SFR	HCD SD Section 2.6.1 FPT_SBT_EXT.1 Extended: Secure Boot, 2.6.1.3 Tests, pg. 59: Add a note in this section saying that the algorithm verification for Root of Trust should be avoided, because authenticity check in Root of Trust should be performed by some kind of immutable code, so the algorithm verification tests should be difficult to perform.	In Progress – Issue was previously submitted to HCD iTC and approved for inclusion in Final Public Draft Fix did not make the deadline so it did not get into v1.0. HIT approved fix previously approved and authorized submittal of TD for this issue.

HCD cPP/SD
HIT RfI Status

Issue #	Title	Issue	Status
HCD-IT #3	Extraneous "selection" in SFR FCS_CKM.4 Cryptographic key destruction in HCD cPP v1.0	Section 5.3.5, FCS_CKM.4 Cryptographic key destruction on page 33: in FCS_CKM.4.1 the last line of the SFR states "] that meets the following: [selection: no standard]." Since the selection has already been made in the cPP, the "selection:" should be deleted.	Complete - Issue was closed with no action taken since it was a duplicate to one of the samples indicated in Issue HCD-IT #7
HCD-IT #4	NIAP APE_ECD.1-5 Evaluation Comments against the HCD cPP	As part of NIAP's review process of the HCD cPP, we performed an evaluation of the APE work units and identified several needing correction. Please see the following comments: APE_ECD.1-5, The evaluator shall examine the extended components definition to determine that each extended functional component uses the existing CC Part 2 components as a model for presentation. – Gave several example	Awaiting Review – HCD-IT #4- #7 are part of the NIAP evaluation of the HCD cPP as part of the certification of the HCD cPP. All the examples and general comments provided by NIAP must be fixed and included in an update to v1.0 as quickly as possible

HCD cPP/SD
HIT RfI Status

Issue #	Title	Issue	Status
HCD-IT #5	NIAP APE_REQ.2-5 Evaluation Comments against the HCD cPP	As part of NIAP's review process of the HCD cPP, we performed an evaluation of the APE work units and identified several needing correction. Please see the following comments: APE_REQ.2-5, The evaluator shall examine the statement of security requirements to determine that all assignment operations are performed correctly. – provides several examples	See HCD-IT #4
HCD-IT #6	NIAP APE_REQ.2-8 Assessment Comments against the HCD cPP	As part of NIAP's review process of the HCD cPP, we performed an evaluation of the APE work units and identified several needing correction. Please see the following comments: APE_REQ.2-8, The evaluator shall examine the statement of security requirements to determine that all refinement operations are performed correctly. -- general inconsistency as to whether an SFR with a refinement in it starts with "Refinement:" or not – several examples noted	See HCD-IT #4

HCD cPP/SD
HIT RfI Status

Issue #	Title	Issue	Status
HCD-IT #7	NIAP APE_REQ.2-7 Assessment of HCD cPP	As part of NIAP's review process of the HCD cPP, we performed an evaluation of the APE work units and identified several needing correction. Please see the following comments: APE_REQ.2-7, The evaluator shall examine the statement of security requirements to determine that all selection operations are performed correctly. -- General inconsistency with regards to whether or not "selection:" prompt is bolded Examples are provided	See HCD-IT #4

HCD iTC
HIT Issues

Scope of HIT

- Theoretically the HIT should be able to handle any issue, so everything is in scope
- Real question is what can the HIT resolve by itself and what does the HIT have to let the full HCD iTC resolve
- The general consensus seems to be:
  - HIT should be able to resolve any issue that involves clarification of existing requirements in either HCD cPP v1.0 or HCD SD v1.0
  - For any issue that involves new content to either the HCD cPP or HCD SD, the HIT should make a recommendation to the full HCD iTC

HCD iTC
HIT Issues

Release Plan

- Is the first release an Errata (1.0a) or v1.0.1
  - Current thought is it should be an Errata to address at a minimum the NIAP comments related to evaluation of the HCD cPP
- When should the first release be published
  - As soon as possible after receipt of all NIAP cPP evaluation comments
- Still need to plan for a possible v1.0.1 of both the HCD cPP and HCD SD in terms of both content and time frame

HCD iTC
Issues Post-Version 1.0 – Release Plan

- Need to develop release plan for future updates of the HCD cPP and HCD SD past v1.0
  - Will have major (v2.0) and minor (1.x) releases first update to HCD cPP and HCD SD will likely be "Errata" releases
  - Timeframe for releases: Current though based on what other iTCs have done is
    - Major releases every 2-3 years
    - Minor releases no later than 18 months after a major release, but sooner if needed.
- What could go into a major or minor release – 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 new versions of ND and FDE cPPs/SDs
  - Requests from Schemes, especially JISEC, ITSCC and NIAP
  - Updates to ISO/IEC 15408 and ISO/IEC 18504
  - New mandates or updated standards from NIAP, NIST, NSA (e.g. CNSA 2.0)
  - Response to new technologies, new crypto algorithms

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

HCD iTC
Issues Post-Version 1.0
Transitioning to CC:2022

- CC v3.1 R5 is the last revision of version 3.1 and may optionally be used for evaluations of Products and Protection Profiles starting no later than the 30th of June 2024
- Security Targets conformant to CC:2022 and based on Protection Profiles certified according to CC v3.1 will be accepted up to the 31st of December 2027
- After 30th of June 2024, re-evaluations and re-assessments based on CC v3.1 evaluations can be started for up to 2 years from the initial certification date
- New initial certifications based on CC v3.1 R5 may be started until 30th of June 2024
  - Product certifications based on CC v3.1 R5 against a PP or PP configuration claiming exact conformance may be started until 31st of December 2025
  - PP authors must update the PP or PP configuration to CC:2022 as soon as possible, and any new or updated PPs or PP configurations published after 30th of June 2024 must be based on CC:2022
- After 30th of June 2024, re-evaluations and re-assessments based on CC v3.1 evaluations can be started for up to 2 years from the initial certification date

HCD iTC
Issues Post-Version 1.0
ND cPP / SD v3.0 Content

Changes in ND cPP / SD v3.0 that could necessitate updates to existing SFRs / Assurance Activities or inclusion of new SFRs / Assurance Activities in updates to HCD cPP / SD:

- Claim conformance to NIAP Functional Package for SSH
- Updates to TLS and DTLS SFRs to incorporate TLS 1.3 and removal of TLS 1.1
- Inclusion of new SFRs under SFRs **FAU_STG_EXT.1 External Audit Trail Storage, FCS_TLSC_EXT.1 TLS Client Protocol Without Mutual Authentication, FCS_TLSS_EXT.1 TLS Server Protocol without Mutual Authentication, FCS_TLSS_EXT.2 TLS Server Support for Mutual Authentication, FCS_DTLSC_EXT.2 DTLS Client Support for Mutual Authentication** and **FPT_STM.1 Reliable Time Stamps**
- Inclusion of new SFRs **FCS_TLSC_EXT.3 TLS Client Support for secure renegotiation (TLSv1.2 only)** and **FCS_TLSS_EXT.3 TLS Server Support for secure renegotiation**
- Inclusion of Optional Security Assurance Requirements for Flaw Remediation (ALC_FLR)
- Added additional requirements to several crypto SFRs like FCS_CKM.4 Cryptographic Key Destruction and FCS_RBG_EXT.1 Random Bit Generation

HCD cPP/SD Content Post-Version 1.0 Potential 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.*
- Incorporate NIAP Functional Package for SSH
- Initial implementation of CNSA 2.0 algorithms
  - Inclusion of SHA-384 and SHA-512 and possible inclusion of LMS as an option likely first steps
- 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 CC:2022 published in November 2022
  - Comparison of CC:2022 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, NIAP and Canada

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

- **Full implementation of CNSA 2.0**
- **Support for any 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, customer requests or government mandates
- Syncing with newer versions of ND and FDE cPPs/SDs

HCD iTC Status
Key Next Steps

- Continue HIT activities for maintaining HCD cPP/SD v1.0
- Agree on the HCD cPP/HCD SD release plan for both v1.0 and updated versions
- Determine the content for and then create the next HCD cPP/SD releases for both v1.0 and an updated version
- 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
Lessons Learned from Initiating the HIT (My Take)

- Starting from scratch, it is important to have someone with experience to learn from; otherwise all you do is flounder around
- "Learning by doing" is the only real way to learn
- When you take a leadership role, you often surprise yourself in the things that you do well and in the things that you don't do so well
- When you are starting up a team, make sure you have a plan. However, make sure the plan is flexible because invariably things will not go as planned
- Maybe my #1 lesson learned so far, if you are the team lead make sure you have a very good vice-lead, because you never know what can happen

Cybersecurity in the United States

US National Cybersecurity Strategy

National Cybersecurity Strategy

- Issued March 1, 2023 from the White House - https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
- Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* and the work performed and reports created in response to that Executive Order laid the groundwork for this National Cyber Strategy
- This National Cyber Strategy provides the first fully articulated US cyber strategy in 15 years
- This strategy explains how the US will:
  - Defend the homeland by protecting networks, systems, functions, and data;
  - Promote American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovation;
  - Preserve peace and security by strengthening the ability of the United States — in concert with allies and partners — to deter and, if necessary, punish those who use cyber tools for malicious purposes; and
  - Expand American influence abroad to extend the key tenets of an open, interoperable, reliable, and secure Internet

National Cybersecurity Strategy Current Landscape

- Rise of the open internet has allowed US competitors and advisories to engage in pernicious economic espionage and malicious cyber activities such as cyber attacks, cyber-enabled economic espionage and trillions of dollars of intellectual property theft , causing significant economic disruption and harm to individuals, commercial and non-commercial interests, and governments across the world
- Public and private entities have struggled to secure their systems as adversaries increase the frequency and sophistication of their malicious cyber activities
- Entities across the US have faced cybersecurity challenges in effectively identifying, protecting, and ensuring resilience of their networks, systems, functions, and data as well as detecting, responding to, and recovering from incidents

National Cybersecurity Strategy Current Landscape

- A cybersecurity strategy to counteract these malicious cyber activities must recognize that:
  - Purely technocratic approach to cyberspace is insufficient to address the nature of these new problems
  - Must impose costs if it hopes to deter malicious cyber actors and prevent further escalation
  - Must be anchored by enduring American values, such as the belief in the power of individual liberty, free expression, free markets, and privacy
  - Must retain the promise of an open, interoperable, reliable, and secure Internet to strengthen and extend our values and protect and ensure economic security for American workers and companies
  - The US is engaged in a continuous competition against strategic adversaries, rogue states, and terrorist and criminal networks
  - The US is vulnerable to peacetime cyber attacks against critical infrastructure, and the risk is growing that these countries will conduct cyber attacks against the United States during a crisis short of war
  - These adversaries are continually developing new and more effective cyber weapons

National Cybersecurity Strategy Four Pillars

I. Protect the American People, the Homeland, and the American Way of Life

- Will require a series of coordinated actions focused on protecting government networks, protecting critical infrastructure, and combating cybercrime

II. Promote American Prosperity

- Need to demonstrate a coherent and comprehensive approach to address challenges that threaten our national security in this increasingly digitized world

III. Preserve Peace through Strength

- Need to issue transformative policies that reflect today's new reality where Cyberspace is no longer treated as a separate category of policy or activity disjointed from other elements of national power

IV. Advance American Influence

- Need to maintain an active international leadership posture to advance American influence and to address an expanding array of threats and challenges to its interests in cyberspace

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

OBJECTIVE: Manage cybersecurity risks to increase the security and resilience of the Nation's information and information systems

Steps

1. Secure Federal Networks and Information by**:**

- **FURTHER CENTRALIZE MANAGEMENT AND OVERSIGHT OF FEDERAL CIVILIAN CYBERSECURITY**
  - Deploy centralized capabilities, tools, and services through DHS where appropriate, and improve oversight and compliance with applicable laws, policies, standards, and directives
- **ALIGN RISK MANAGEMENT AND INFORMATION TECHNOLOGY ACTIVITIES**
  - The Administration, through OMB and DHS, will guide and direct risk management actions across Federal civilian departments and agencies, and CIOs will be empowered to take a proactive leadership role in assuring IT procurement decisions assign the proper priority to securing networks and data

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

1. **Secure Federal Networks and Information** by**:**
   - **IMPROVE FEDERAL SUPPLY CHAIN RISK MANAGEMENT**
     - Integrate supply chain risk management into agency procurement and risk management processes in accordance with federal requirements that are consistent with industry best practices
   - **STRENGTHEN FEDERAL CONTRACTOR CYBERSECURITY**
     - Ensure, where appropriate, that Federal contractors receive and use all relevant and shareable threat and vulnerability information
   - **ENSURE THE GOVERNMENT LEADS IN BEST AND INNOVATIVE PRACTICES**
     - Be a leader in developing and implementing standards and best practices in new and emerging areas such as quantum computing

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

2. Support Critical Infrastructure by**:**

- **REFINE ROLES AND RESPONSIBILITIES**
  - Identify and bridge existing gaps in responsibilities and coordination among Federal and non-Federal incident response efforts and promote more routine training, exercises, and coordination
- **PRIORITIZE ACTIONS ACCORDING TO IDENTIFIED NATIONAL RISKS**
  - Prioritize risk-reduction activities across seven key areas: national security, energy and power, banking and finance, health and safety, communications, information technology, and transportation
- **LEVERAGE INFORMATION AND COMMUNICATIONS TECHNOLOGY PROVIDERS AS CYBERSECURITY ENABLERS**
  - Promote an adaptable, sustainable, and secure technology supply chain that supports security based on best practices and standards

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

2. Support Critical Infrastructure by**:**

- **PROTECT OUR DEMOCRACY**
  - Coordinate the development of cybersecurity standards and guidance to safeguard the electoral process and the tools that deliver a secure system
- **INCENTIVIZE CYBERSECURITY INVESTMENTS**
  - Work with private and public sector entities to promote understanding of cybersecurity risk so they make more informed risk-management decisions, invest in appropriate security measures, and realize benefits from those investments
- **PRIORITIZE NATIONAL RESEARCH AND DEVELOPMENT INVESTMENTS**
  - Align investments to the priorities, which will focus on building new cybersecurity approaches that use emerging technologies, improving information-sharing and risk management related to cross-sector interdependencies, and building resilience to large-scale or long-duration disruptions

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

2. Support Critical Infrastructure by**:**

- **IMPROVE TRANSPORTATION AND MARITIME CYBERSECURITY**
  - Clarify maritime cybersecurity roles and responsibilities; promote enhanced mechanisms for international coordination and information sharing; and accelerate the development of next-generation cyber-resilient maritime infrastructure
- **IMPROVE SPACE CYBERSECURITY**
  - Enhance efforts to protect our space assets and support infrastructure from evolving cyber threats

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

3. Combat Cybercrime and Improve Incident Reporting by**:**

- **IMPROVE INCIDENT REPORTING AND RESPONSE**
  - Encourage reporting of intrusions and theft of data by all victims, especially critical infrastructure partners
- **MODERNIZE ELECTRONIC SURVEILLANCE AND COMPUTER CRIME LAWS**
  - Work with the Congress to update electronic surveillance and computer crime statutes to enhance law enforcement's capabilities to lawfully gather necessary evidence of criminal activity, disrupt criminal infrastructure through civil injunctions, and impose appropriate consequences upon malicious cyber actors
- **REDUCE THREATS FROM TRANSNATIONAL CRIMINAL ORGANIZATIONS IN CYBERSPACE**
  - Advocate for law enforcement to have effective legal tools to investigate and prosecute transnational criminal groups and modernized organized crime statutes for use against computer hacking

National Cybersecurity Strategy
Pillar I -- Protect the American People, the Homeland, and the American Way of Life

Steps

3. Combat Cybercrime and Improve Incident Reporting by**:**

- **IMPROVE APPREHENSION OF CRIMINALS LOCATED ABROAD**
  - Identify gaps and potential mechanisms for bringing foreign based cyber criminals to justice
- **STRENGTHEN PARTNER NATIONS' LAW ENFORCEMENT CAPACITY TO COMBAT CRIMINAL CYBER ACTIVITY**
  - Continue building cybercrime-fighting capacity that facilitates stronger international law enforcement cooperation

National Cybersecurity Strategy
Pillar II – Promote American Prosperity

OBJECTIVE: Preserve United States influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency

Steps

1. Foster a Vibrant and Resilient Digital Economy by**:**

- **INCENTIVIZE AN ADAPTABLE AND SECURE TECHNOLOGY MARKETPLACE**
  - Collaborate with international partners to promote open, industry-driven standards with government support, as appropriate, and risk-based approaches to address cybersecurity challenges
- **PRIORITIZE INNOVATION**
  - Promote implementation and continuous updating of standards and best practices that deter and prevent current and evolving threats and hazards in all domains of the cyber ecosystem

National Cybersecurity Strategy
Pillar II – Promote American Prosperity

Steps

1. Foster a Vibrant and Resilient Digital Economy by**:**

- **INVEST IN NEXT GENERATION INFRASTRUCTURE**
  - Facilitate the accelerated development and rollout of next-generation telecommunications and information communications infrastructure in the US
  - Examine the use of emerging technologies, such as artificial intelligence and quantum computing, while addressing risks inherent in their use and application
- **PROMOTE THE FREE FLOW OF DATA ACROSS BORDERS**
  - Continue to work with international counterparts to promote open, industry driven standards, innovative products, and risk-based approaches that permit global innovation and the free flow of data
- **MAINTAIN UNITED STATES LEADERSHIP IN EMERGING TECHNOLOGIES**
  - Make a concerted effort to protect cutting edge technologies, including from theft by our adversaries, support those technologies' maturation, and, where possible, reduce United States companies' barriers to market entry

National Cybersecurity Strategy
Pillar II – Promote American Prosperity

Steps

1. Foster a Vibrant and Resilient Digital Economy by**:**

- **PROMOTE FULL-LIFECYCLE CYBERSECURITY**
  - Promote full-lifecycle cybersecurity, pressing for strong, default security settings, adaptable, upgradeable products, and other best practices built in at the time of product delivery

2. Foster and Protect United States Ingenuity by**:**

- **UPDATE MECHANISMS TO REVIEW FOREIGN INVESTMENT AND OPERATION IN THE UNITED STATES**
  - Formalizing and streamlining the review of Federal Communications Commission referrals for telecommunications licenses
- **MAINTAIN A STRONG AND BALANCED INTELLECTUAL PROPERTY PROTECTION SYSTEM**
  - Continue to help foster a global intellectual property rights system that provides incentives for innovation through the protection and enforcement of intellectual property rights

National Cybersecurity Strategy
Pillar II – Promote American Prosperity

Steps

2. Foster and Protect United States Ingenuity by**:**

- **PROTECT THE CONFIDENTIALITY AND INTEGRITY OF AMERICAN IDEAS**
  - Work against the illicit appropriation of public and private sector technology and technical knowledge by foreign competitors, while maintaining an investor-friendly climate

3. Develop a Superior Cybersecurity Workforce by**:**

- **BUILD AND SUSTAIN THE TALENT PIPELINE**
  - Continue to invest in and enhance programs that build the domestic talent pipeline, from primary through postsecondary education
- **EXPAND RE-SKILLING AND EDUCATIONAL OPPORTUNITIES FOR AMERICA'S WORKERS**
  - Work with the Congress to promote and reinvigorate educational and training opportunities to develop a robust cybersecurity workforce

National Cybersecurity Strategy
Pillar II – Promote American Prosperity

Steps

3. Develop a Superior Cybersecurity Workforce by**:**

- **ENHANCE THE FEDERAL CYBERSECURITY WORKFORCE**
  - Continue to use the National Initiative for Cybersecurity Education (NICE) Framework to support policies allowing for a standardized approach for identifying, hiring, developing, and retaining a talented cybersecurity workforce
- **USE EXECUTIVE AUTHORITY TO HIGHLIGHT AND REWARD TALENT**
  - Implement actions to prepare, grow, and sustain a workforce that can defend and bolster America's critical infrastructure and innovation base

National Cybersecurity Strategy
Pillar III – Preserve Peace Through Strength

OBJECTIVE: Identify, counter, disrupt, degrade, and deter behavior in cyberspace that is destabilizing and contrary to national interests, while preserving United States overmatch in and through cyberspace

Steps

1. Enhance Cyber Stability through Norms of Responsible State Behavior by**:**

- **ENCOURAGE UNIVERSAL ADHERENCE TO CYBER NORMS**
  - Encourage other nations to publicly affirm International law and voluntary non-binding norms of responsible state behavior in cyberspace) through enhanced outreach and engagement in multilateral for a

2. Attribute and Deter Unacceptable Behavior in Cyberspace by**:**

- **LEAD WITH OBJECTIVE, COLLABORATIVE INTELLIGENCE**
  - Lead the world in the use of all-source cyber intelligence to drive the identification and attribution of malicious cyber activity that threatens United States national interests

National Cybersecurity Strategy
Pillar III – Preserve Peace Through Strength

Steps

2. Attribute and Deter Unacceptable Behavior in Cyberspace by**:**

- **IMPOSE CONSEQUENCES**
  - Develop swift and transparent consequences, which we will impose consistent with our obligations and commitments to deter future bad behavior
- **BUILD A CYBER DETERRENCE INITIATIVE**
  - Launch an international Cyber Deterrence Initiative to build broader coalition of like-minded states and develop tailored strategies to ensure adversaries understand the consequences of their malicious cyber behavior
- **COUNTER MALIGN CYBER INFLUENCE AND INFORMATION OPERATIONS**
  - Use all appropriate tools of national power to expose and counter the flood of online malign influence and information campaigns and non-state propaganda and disinformation

National Cybersecurity Strategy
Pillar IV – Advance American Influence

OBJECTIVE: Preserve the long-term openness, interoperability, security, and reliability of the Internet, which supports and is reinforced by United States interests

Steps

1. Promote an Open, Interoperable, Reliable, and Secure Internet by**:**

- **PROTECT AND PROMOTE INTERNET FREEDOM**
  - Encourage other countries to advance Internet freedom through venues such as the Freedom Online Coalition, of which the United States is a founding member

    Note: 'Internet Freedom' in this context is defined as online exercise of human rights and fundamental freedoms — such as the freedoms of expression, association, peaceful assembly, religion or belief, and privacy rights online — regardless of frontiers or medium. By extension, Internet freedom also supports the free flow of information online that enhances international trade and commerce, fosters innovation, and strengthens both national and international security

National Cybersecurity Strategy
Pillar IV – Advance American Influence

Steps

1. Promote an Open, Interoperable, Reliable, and Secure Internet by**:**

- **WORK WITH LIKE-MINDED COUNTRIES, INDUSTRY, ACADEMIA, AND CIVIL SOCIETY**
  - Continue to work with like-minded countries, industry, civil society, and other stakeholders to advance human rights and Internet freedom globally and to counter authoritarian efforts to censor and influence Internet development
- **PROMOTE A MULTI-STAKEHOLDER MODEL OF INTERNET GOVERNANCE**
  - Continue to actively participate in global efforts to ensure that the multi-stakeholder model of Internet governance (characterized by transparent, bottom-up, consensus-driven processes) prevails against attempts to create state-centric frameworks that would undermine openness and freedom, hinder innovation, and jeopardize the functionality of the Internet

National Cybersecurity Strategy
Pillar IV – Advance American Influence

Steps

1. Promote an Open, Interoperable, Reliable, and Secure Internet by**:**

- **PROMOTE INTEROPERABLE AND RELIABLE COMMUNICATIONS INFRASTRUCTURE AND INTERNET CONNECTIVITY**
  - Promote communications infrastructure and Internet connectivity that is open, interoperable, reliable, and secure
- **PROMOTE AND MAINTAIN MARKETS FOR UNITED STATES INGENUITY WORLDWIDE**
  - Advise on infrastructure deployments, innovation, risk management, policy, and standards to further the global Internet's reach and to ensure interoperability, security, and stability

2. Build International Cyber Capacity by**:**

- **ENHANCE CYBER CAPACITY BUILDING EFFORTS**
  - Aggressively expand efforts to share automated and actionable cyber threat information, enhance cybersecurity coordination, and promote analytical and technical exchange

CISA (Cybersecurity and Infrastructure Security Agency) Strategic Plan 2023 - 2025

CISA Strategic Plan 2023 – 2025 Purpose

https://www.cisa.gov/sites/default/files/2023-01/StrategicPlan_20220912-V2_508c.pdf

- Communicate the Cybersecurity and Infrastructure Security Agency's (CISA) mission and vision
- Promote unity of effort across the agency and our partners, and defines success for CISA as an agency
- Describe the stakeholder, policy, and operational context in which CISA must perform and present the strategic changes CISA will make to better execute our vital mission over the next three years
- Builds on and aligns with the *United States Department of Homeland Security Strategic Plan for Fiscal Years 2020 – 2024*

CISA Strategic Plan 2023 – 2025
CISA Core Values

- **Collaboration** - We will approach every engagement as an opportunity to build trust with our teammates, our partners, and our customers
- **Innovation** - We must move with creativity and agility at the speed of ideas to stay ahead of threats to our nation and our way of life, and we must be grounded in the strength of our resilience
- **Service** - Our commitment is a calling to protect and defend the infrastructure Americans rely on every hour of every day
- **Accountability** - We will model the behavior we want to see in others; we will hold ourselves and our teammates responsible for our actions; and we will empower our workforce through trust, transparency, and radical honesty

CISA Strategic Plan 2023 – 2025 Goals

- **Cyber Defense** - SPEARHEAD THE NATIONAL EFFORT TO ENSURE DEFENSE AND RESILIENCE OF CYBERSPACE
- **Risk Reduction and Resilience** - REDUCE RISKS TO, AND STRENGTHEN RESILIENCE OF, AMERICA'S CRITICAL INFRASTRUCTURE
- **Operational Collaboration** - STRENGTHEN WHOLE- OF-NATION OPERATIONAL COLL ABORATION AND INFORMATION SHARING
- **Agency Unification** - UNIFY AS ONE CISA THROUGH INTEGRATED FUNCTIONS, CAPABILITIES, AND WORKFORCE

CISA Strategic Plan 2023 – 2025
Goal 1 - Cyber Defense

Objective 1.1 ENHANCE THE ABILITY OF FEDERAL SYSTEMS TO WITHSTAND CYBERATTACKS AND INCIDENTS

- Driving and facilitating the adoption of modern, secure, and resilient technologies

Objective 1.2 INCREASE CISA'S ABILITY TO ACTIVELY DETECT CYBER THREATS TARGETING AMERICA'S CRITICAL INFRASTRUCTURE AND CRITICAL NETWORKS

- Will advance our capability to actively detect threats across federal and SLTT networks while working with industry partners to enhance our understanding of threats targeting private networks

Objective 1.3 DRIVE THE DISCLOSURE AND MITIGATION OF CRITICAL CYBER VULNERABILITIES

- Along with our partners, will enable timely and coordinated vulnerability disclosure, provide recommendations, and amplify appropriate mitigation countermeasures using relevant channels and mechanisms

Objective 1.4 ADVANCE THE CYBERSPACE ECOSYSTEM TO DRIVE SECURITY-BY-DEFAULT

- Foster the development and adoption of state-of-the-art network defense and cyber operations tools, services, and capabilities to drive security-by-default in the technology ecosystem

CISA Strategic Plan 2023 – 2025
Goal 2 - Risk Reduction and Resilience

Objective 2.1 EXPAND VISIBILITY OF RISKS TO INFRASTRUCTURE, SYSTEMS, AND NETWORKS

- Need to deepen our insights into the nation's cyber and physical critical infrastructure assets and systems, as well as identifying the potential and future sources of risk that could impact that infrastructure

Objective 2.2 ADVANCE CISA'S RISK ANALYTIC CAPABILITIES AND METHODOLOGIES

- Must mature CISA's risk analysis capabilities and methodologies to promote in-depth understanding of the risks we face

Objective 2.3 ENHANCE CISA'S SECURITY AND RISK MITIGATION GUIDANCE AND IMPACT

- Will issue authoritative guidance to drive effective IT network risk management

Objective 2.4 BUILD GREATER STAKEHOLDER CAPACITY IN INFRASTRUCTURE AND NETWORK SECURITY AND RESILIENCE

- Will deliver impactful capabilities and services to meet our stakeholders' most pressing and evolving physical security challenges, which include insider threats, active shooter preparedness, bombing prevention, and security in public gathering places

CISA Strategic Plan 2023 – 2025
Goal 2 - Risk Reduction and Resilience

Objective 2.5 INCREASE CISA'S ABILITY TO RESPOND TO THREATS AND INCIDENTS

- Must bolster and expand our headquarters and regional capacity to support our stakeholders and interagency partners following physical threats and incidents

Objective 2.6 SUPPORT RISK MANAGEMENT ACTIVITIES FOR ELECTION INFRASTRUCTURE

- Be the federal government's hub for understanding and characterizing risks to election infrastructure and ensuring election officials and their private sector partners have the information they need to manage risk to their systems

CISA Strategic Plan 2023 – 2025
Goal 3 - Operational Cooperation

Objective 3.1 OPTIMIZE COLLABORATIVE PLANNING AND IMPLEMENTATION OF STAKEHOLDER ENGAGEMENTS AND PARTNERSHIP ACTIVITIES

- Must plan, prioritize, and coordinate stakeholder engagements within our agency, SRMAs, and across the broader stakeholder community

Objective 3.2 FULLY INTEGRATE REGIONAL OFFICES INTO CISA'S OPERATIONAL COORDINATION

- Will establish processes for coordinating engagement activities between HQ divisions and regions and mutually support operational relationship management

Objective 3.3 STREAMLINE STAKEHOLDER ACCESS TO AND USE OF APPROPRIATE CISA PROGRAMS, PRODUCTS, AND SERVICES

- Wherever possible and suitable, will offer our customers tailored product information, access, and delivery, based on their specific needs and circumstances; to this end, our catalog of resources will be consistently available, accurate, tailorable, engaging, and easy to access

CISA Strategic Plan 2023 – 2025
Goal 3 - Operational Cooperation

Objective 3.4 ENHANCE INFORMATION SHARING WITH CISA'S PARTNERSHIP BASE

- Must enhance multidirectional communications with external partners, including timely incident reporting and the sharing of threats and vulnerabilities, intelligence and intelligence requirements, as well as other information and data

Objective 3.5 INCREASE INTEGRATION OF STAKEHOLDER INSIGHTS TO INFORM CISA PRODUCT DEVELOPMENT AND MISSION DELIVERY

- Will increase integration of stakeholder insights, information, and data to assist in decision making and the prioritization, development, modification, and tailoring of our products, services, and areas of focus

CISA Strategic Plan 2023 – 2025
Goal 4 - Agency Unification

Objective 4.1 STRENGTHEN AND INTEGRATE CISA GOVERNANCE, MANAGEMENT, AND PRIORITIZATION

- Will work to delineate lines of effort and assign organizational and/or individual responsibility to drive collective decision making, and document and integrate processes to ensure standardization and utilization of best practices

Objective 4.2 OPTIMIZE CISA BUSINESS OPERATIONS TO BE MUTUALLY SUPPORTIVE ACROSS ALL DIVISIONS

- Will streamline existing operations and adopt agile, new technologies that will enable customer service and improved timely, modern, and secure services

Objective 4.3 CULTIVATE AND GROW CISA'S HIGH-PERFORMING WORKFORCE

- Will implement a world-class talent ecosystem that spans recruiting, hiring, training, recognition, advancement, retention, and succession planning

Objective 4.4 ADVANCE CISA'S CULTURE OF EXCELLENCE

- Our culture will be incorporated in our day-to-day tasks, mission-enabling functions, service to our partners and stakeholders, and in our everyday behaviors

HCD Security Guidelines

Liaison Status

Trusted Computing Group (TCG)

- **Next TCG Members Meetings**
  - **TCG Hybrid F2F (Berlin, Germany) – 27-29 June 2023 – Ira to call in**
  - **TCG Hybrid F2F (Kirkland, WA) – 24-26 October 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 – public review April 2023***
  - ***TCG TPM 2.0 Mobile Common Profile – work-in-progress for review Q3/Q4 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 MARS API v1 – published May 2023***
  - ***TCG Mobile Reference Architecture v2 – public review April 2023***
  - ***TCG DICE Protection Environment – public review April 2023***
  - ***TCG EK Credential Profile for TPM 2.0 – published March 2023***
  - ***TCG MARS FAQ – published February 2023***
  - ***TCG Measurement and Attestation RootS (MARS) Library – published January 2023***

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

- **Next IETF Members Meetings**
  - **IETF 117 Hybrid F2F (San Francisco, CA) – 24-28 July 2023 – Ira to call in**
  - **IETF 118 Hybrid F2F (Prague, Czech Republic) – 6-10 November 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 TLS Encrypted Client Hello – draft-16 – April 2023**
    https://datatracker.ietf.org/doc/draft-ietf-tls-esni/
  - **IETF IANA Registry Updates for TLS/DTLS – draft-04 – March 2023 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8447bis/
  - **IETF TLS 13 – draft-07 – March 2023 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-tls-rfc8446bis/
  - **Compact ECDHE and ECDSA Encodings for TLS 1.3 – March 2023**
    https://datatracker.ietf.org/doc/draft-mattsson-tls-compact-ecc/
  - **IETF Compact TLS 1.3 – draft-08 – March 2023**
    https://datatracker.ietf.org/doc/draft-ietf-tls-ctls/
  - **IETF Deprecating Obsolete Key Exchange Methods in TLS 1.2 – draft-02 – March 2023**
    https://datatracker.ietf.org/doc/draft-ietf-tls-deprecate-obsolete-kex/
  - **IETF Hybrid key exchange in TLS 1.3 – draft-06 – February 2023**
    https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
  - **IETF Delegated Credentials for (D)TLS – draft-15 – RFC Editor / Auth 48**
    https://datatracker.ietf.org/doc/draft-ietf-tls-subcerts/

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

- **Security Automation and Continuous Monitoring (SACM)**
  - **IETF Software Inventory Message and Attributes for PA-TNC – RFC 8412 – July 2018**
    https://datatracker.ietf.org/doc/rfc8412/
  - **IETF Concise Software Identifiers – draft-24 – February 2023 – RFC Editor / Auth 48**
    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 Gordian dCBOR: Deterministic CBOR – draft-01 – May 2023**
    https://datatracker.ietf.org/doc/draft-mcnally-deterministic-cbor/
  - **IETF Envelope Structured Data Format – draft-02 – May 2023**
    https://datatracker.ietf.org/doc/draft-mcnally-envelope/
  - **IETF CBOR Tags for Time, Duration, and Period – draft-05 – March 2023 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-time-tag/
  - **IETF App-Oriented Literals in CBOR Ext Diag Notation – draft-02 – March 2023**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-edn-literals/
  - **IETF Feature Freezer for CDDL – draft-11 – March 2023**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-freezer/
  - **IETF CDDL 2.0 -- a draft plan - draft-02 - March 2023**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-2-draft/
  - **IETF CDDL Module Structure – draft-00 – March 2023**
    https://datatracker.ietf.org/doc/draft-bormann-cbor-cddl-modules/
  - **IETF Packed CBOR – draft-08 – January 2023 – WG Last Call**
    https://datatracker.ietf.org/doc/draft-ietf-cbor-packed/

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 Proximate Location Claim – draft-00 – March 2023**
    https://datatracker.ietf.org/doc/draft-mandyam-rats-proxlocclaim/
  - **IETF Epoch Markers – draft-04 – March 2023**
    https://datatracker.ietf.org/doc/draft-birkholz-rats-epoch-markers/
  - **IETF Direct Anonymous Attestation for RATS – draft-03 – March 2023**
    https://datatracker.ietf.org/doc/draft-ietf-rats-daa/
  - **IETF EAT Media Types – draft-02 – March 2023**
    https://datatracker.ietf.org/doc/draft-ietf-rats-eat-media-type/
  - **IETF Attestation Event Stream Subscription – draft-03 – March 2023**
    https://datatracker.ietf.org/doc/draft-ietf-rats-network-device-subscription/
  - **IETF Reference Interaction Models for RATS – draft-07 – March 2023**
    https://datatracker.ietf.org/doc/draft-ietf-rats-reference-interaction-models/
  - **IETF CoRIM Profile for ARM PSA – draft-02 – March 2023**
    https://datatracker.ietf.org/doc/draft-fdb-rats-psa-endorsements/
  - **IETF Concise Reference Integrity Manifest (CoRIM) – draft-01 – March 2023**
    https://datatracker.ietf.org/doc/draft-ietf-rats-corim/
  - **IETF RATS Endorsements: CORIM vs EAT – draft-00 – March 2023**
    https://datatracker.ietf.org/doc/draft-dthaler-rats-endorsements/
  - **IETF RATS Conceptual Messages Wrapper – draft-02 – March 2023**
    https://datatracker.ietf.org/doc/draft-ftbs-rats-msg-wrap/
  - **IETF Attestation Results for Secure Interactions – draft-04 – March 2023**
    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 Two-Round Threshold Schnorr Sigs with FROST – draft-13 – May 2023 – to IRTF Chair**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-frost/
  - **IRTF Galois Counter Mode with Secure Short Tags (GCM-SST) – draft-00 – May 2023**
    https://datatracker.ietf.org/doc/draft-mattsson-cfrg-aes-gcm-sst/
  - **IRTF X25519 Kyber768D Hybrid Post-Quantum KEM for HPKE – draft-02 – May 2023**
    https://datatracker.ietf.org/doc/draft-westerbaan-cfrg-hpke-xyber768d00/
  - **IRTF NTRU Key Encapsulation – draft-01 – May 2023**
    https://datatracker.ietf.org/doc/draft-fluhrer-cfrg-ntru/
  - **IRTF AEGIS family of authenticated encryption algorithms – draft-03 – April 2023**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-aegis-aead/
  - **IRTF Ristretto255 and Decaf448 Groups – draft-07 – April 2023 – to IRTF Chair**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-ristretto255-decaf448/
  - **IRTF RSA Blind Signatures - draft-12 - April 2023 – to IRTF Chair**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-rsa-blind-signatures/
  - **IRTF Oblivious Pseudorandom Functions (OPRFs) – February 2023 – RFC Editor**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-voprf/
  - **IRTF Verifiable Random Functions (VRFs) – draft-15 – August 2022 – RFC Editor / Auth 48**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-vrf/
  - **IRTF Hashing to Elliptic Curves – draft-16 – June 2022 – RFC Editor / Auth 48**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-hash-to-curve/
  - **IRTF SPAKE2, a PAKE – draft-26 – February 2022 – RFC Editor / Auth 48**
    https://datatracker.ietf.org/doc/draft-irtf-cfrg-spake2/

Next Steps – IDS WG

- Next IDS WG Meeting– June 1, 2023
- Next IDS Face-to-Face Meeting likely August 10, 2023 at PWG August 2023 F2F
- Start looking at involvement in some of these other standards activities individually and maybe as a WG

Note: The full presentation of the US National Cybersecurity Strategy can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/National Cybersecurity Strategy.pdf

The full presentation of the CISA Strategic Plan 2023 – 2025 can be found at https://ftp.pwg.org/pub/pwg/ids/Presentation/CISA Strategic Plan 2023 - 2025.pdf

Backup

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 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