Office of Information Security
Securing One HHS

2023 IHS Partnership Conference

Office of Information Security
HHS Cybersecurity Program

August 23, 2023

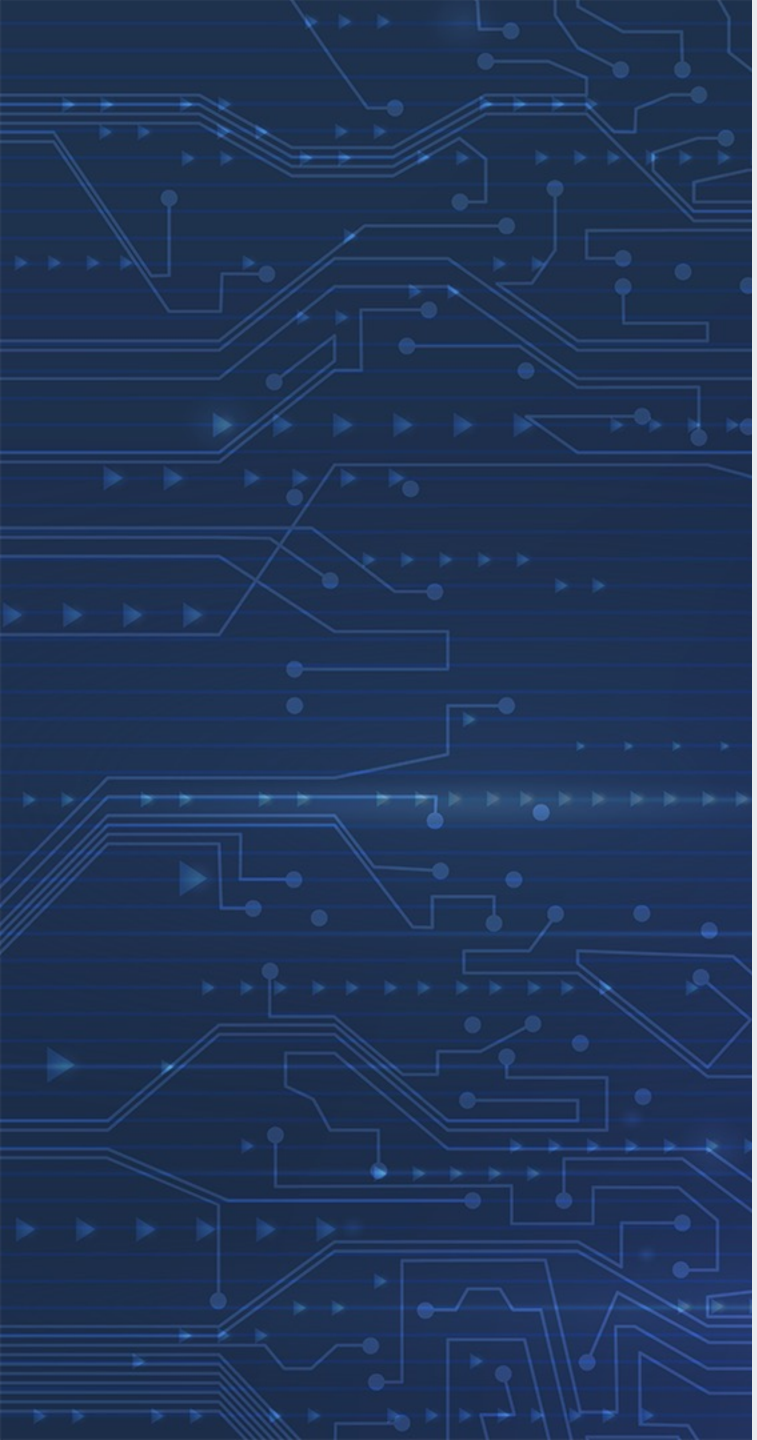
HHS Cybersecurity Program Overview

HHS' enterprise-wide information security and privacy program were launched in the fiscal year 2003, to help protect HHS against potential information technology (IT) threats and vulnerabilities.

The HHS Cybersecurity Program ensures compliance with federal mandates and legislation, including FISMA and the President's Management Agenda.

The Program plays an important role in protecting HHS' ability to provide mission-critical operations. In addition, the HHS Cybersecurity Program is the cornerstone of the HHS IT Strategic Plan and an enabler for e-government success.

HHS SECURITY DESIGN & INNOVATION
HHS OFFICE OF INFORMATION SECURITY
CLOUD SECURITY TEAM
HHS CyberCARE
Communication, Awareness, Response, & Education
ALIGNING HEALTH CARE INDUSTRY SECURITY APPROACHES
HHS 405(d)
HHS OFFICE OF INFORMATION SECURITY
SECURITY OPERATIONS DIVISION
US DHHS OFFICE OF INFORMATION SECURITY BUSINESS OPERATIONS DIVISION
HEALTH SECTOR CYBERSECURITY COORDINATION CENTER
HC3
CDM
Continuous Diagnostics & Mitigation



Agenda

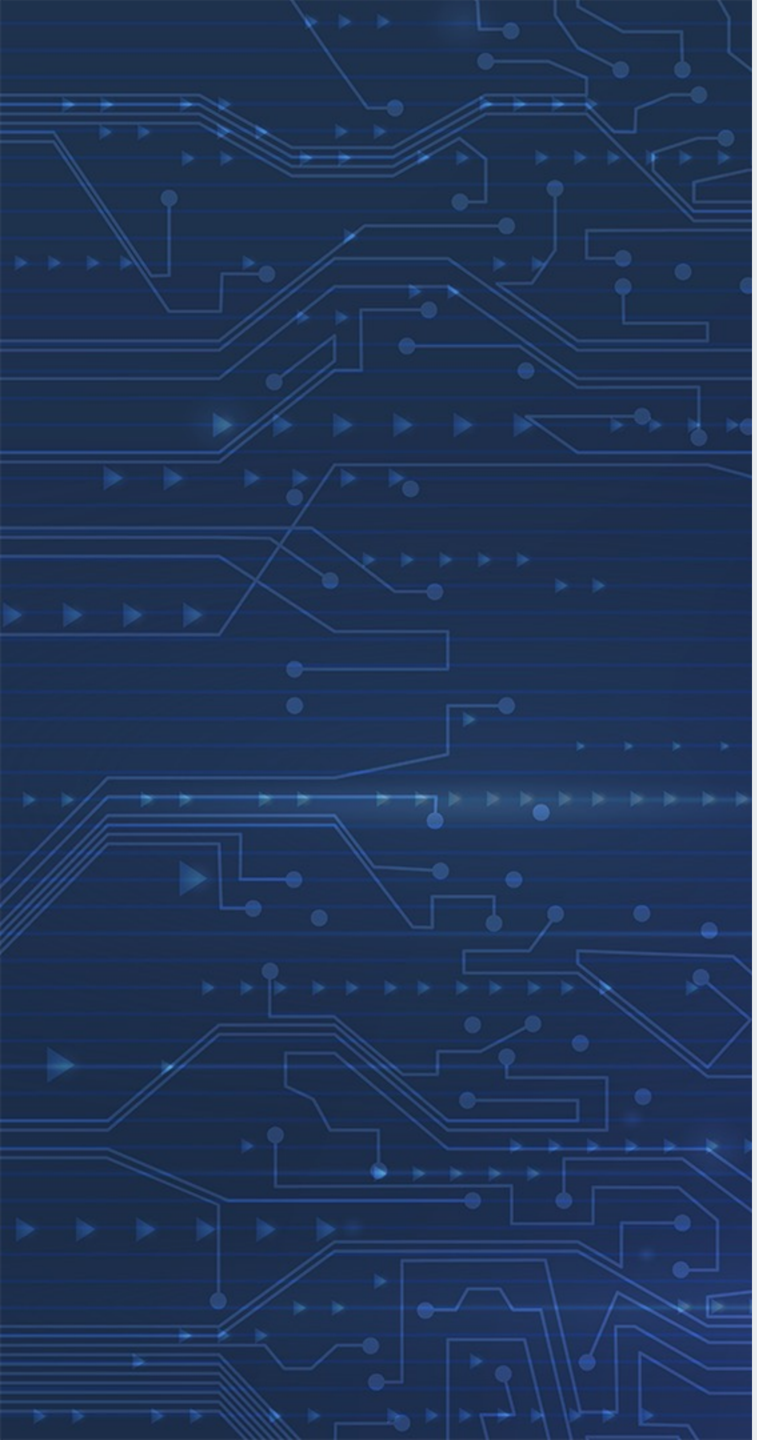
HHS Cybersecurity Initiatives:

- Zero Trust (Speaker: Evan Miller)
- M-23-02, Migrating to Post Quantum Cryptography (Speaker: Conrad Bovell)

Embracing Rapid Cybersecurity Advancements to Defend Health Networks (Speaker: Rahul Gaitonde)

Best Practices for Healthcare Cybersecurity Governance in the Artificial Intelligence (AI) Age:

- HHS 405(d) Program- (Speaker: Nick Rodriguez)
- AI- (Speaker: Rahul Gaitonde)



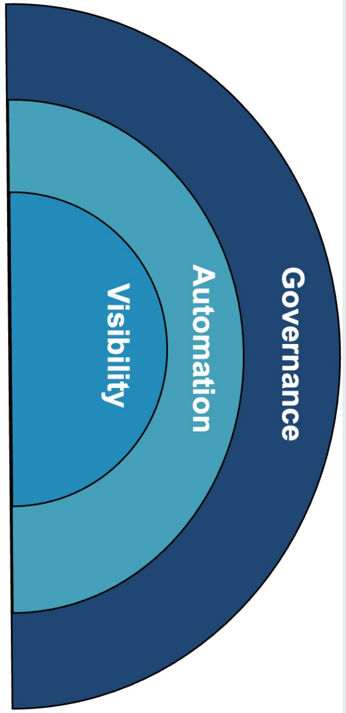
What is Zero Trust?

Speaker: Evan Miller

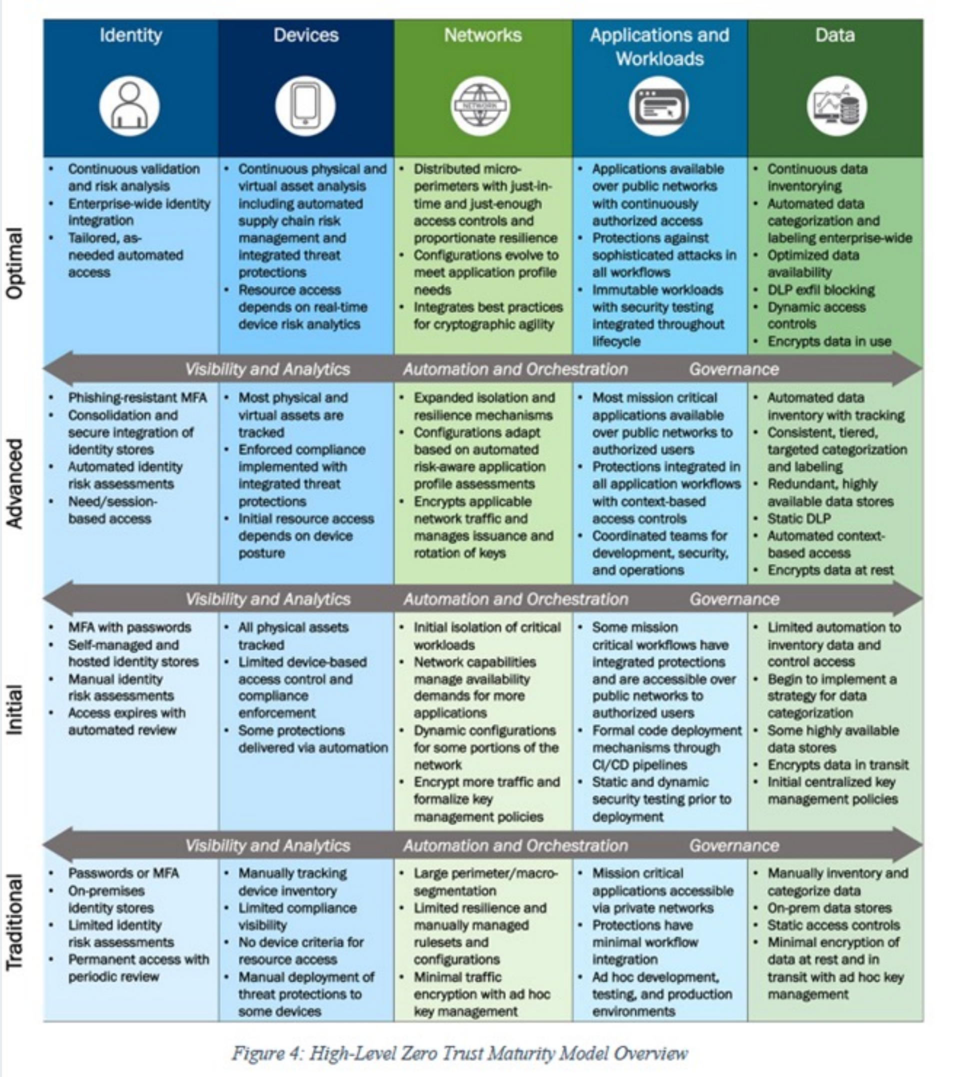
OMB/CISA Zero Trust Vision

Zero trust requires an organization to be technically agile across multiple disciplines; integrate operational capabilities which have historically acted independently; and centrally manage comprehensive inventories to make context-aware access control decisions in real time.

1	Identity	Federal staff have enterprise-managed accounts, allowing them to access everything they need to do their job while remaining reliably protected from even targeted, sophisticated phishing attacks.
2	Devices	The devices that Federal staff use to do their jobs are consistently tracked and monitored, and the security posture of those devices is taken into account when granting access to internal resources.
3	Networks	Agency systems are isolated from each other, and the network traffic flowing between and within them is reliably encrypted.
4	Applications & Workloads	Enterprise applications are tested internally and externally, and can be made available to staff securely over the internet.
5	Data	Federal security teams and data teams work together to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information.



Zero Trust Capabilities are Built over Time



	Identity	Devices	Networks	Applications and Workloads	Data
Optimal	• Continuous validation and risk analysis • Enterprise-wide identity integration • Tailored, as-needed automated access	• Continuous physical and virtual asset analysis including automated supply chain risk management and integrated threat protections • Resource access depends on real-time device risk analytics	• Distributed micro-perimeters with just-in-time and just-enough access controls and proportionate resilience • Configurations evolve to meet application profile needs • Integrates best practices for cryptographic agility	• Applications available over public networks with continuously authorized access • Protections against sophisticated attacks in all workflows • Immutable workloads with security testing integrated throughout lifecycle	• Continuous data inventorying • Automated data categorization and labeling enterprise-wide • Optimized data availability • DLP exfil blocking • Dynamic access controls • Encrypts data in use
		Visibility and Analytics	Automation and Orchestration		Governance
Advanced	• Phishing-resistant MFA • Consolidation and secure integration of identity stores • Automated identity risk assessments • Need/session-based access	• Most physical and virtual assets are tracked • Enforced compliance implemented with integrated threat protections • Initial resource access depends on device posture	• Expanded isolation and resilience mechanisms • Configurations adapt based on automated risk-aware application profile assessments • Encrypts applicable network traffic and manages issuance and rotation of keys	• Most mission critical applications available over public networks to authorized users • Protections integrated in all application workflows with context-based access controls • Coordinated teams for development, security, and operations	• Automated data inventory with tracking • Consistent, tiered, targeted categorization and labeling • Redundant, highly available data stores • Static DLP • Automated context-based access • Encrypts data at rest
		Visibility and Analytics	Automation and Orchestration		Governance
Initial	• MFA with passwords • Self-managed and hosted identity stores • Manual identity risk assessments • Access expires with automated review	• All physical assets tracked • Limited device-based access control and compliance enforcement • Some protections delivered via automation	• Initial isolation of critical workloads • Network capabilities manage availability demands for more applications • Dynamic configurations for some portions of the network • Encrypt more traffic and formalize key management policies	• Some mission critical workflows have integrated protections and are accessible over public networks to authorized users • Formal code deployment mechanisms through CI/CD pipelines • Static and dynamic security testing prior to deployment	• Limited automation to inventory data and control access • Begin to implement a strategy for data categorization • Some highly available data stores • Encrypts data in transit • Initial centralized key management policies
		Visibility and Analytics	Automation and Orchestration		Governance
Traditional	• Passwords or MFA • On-premises identity stores • Limited identity risk assessments • Permanent access with periodic review	• Manually tracking device inventory • Limited compliance visibility • No device criteria for resource access • Manual deployment of threat protections to some devices	• Large perimeter/macro-segmentation • Limited resilience and manually managed rulesets and configurations • Minimal traffic encryption with ad hoc key management	• Mission critical applications accessible via private networks • Protections have minimal workflow integration • Ad hoc development, testing, and production environments	• Manually inventory and categorize data • On-prem data stores • Static access controls • Minimal encryption of data at rest and in transit with ad hoc key management

Figure 4: High-Level Zero Trust Maturity Model Overview

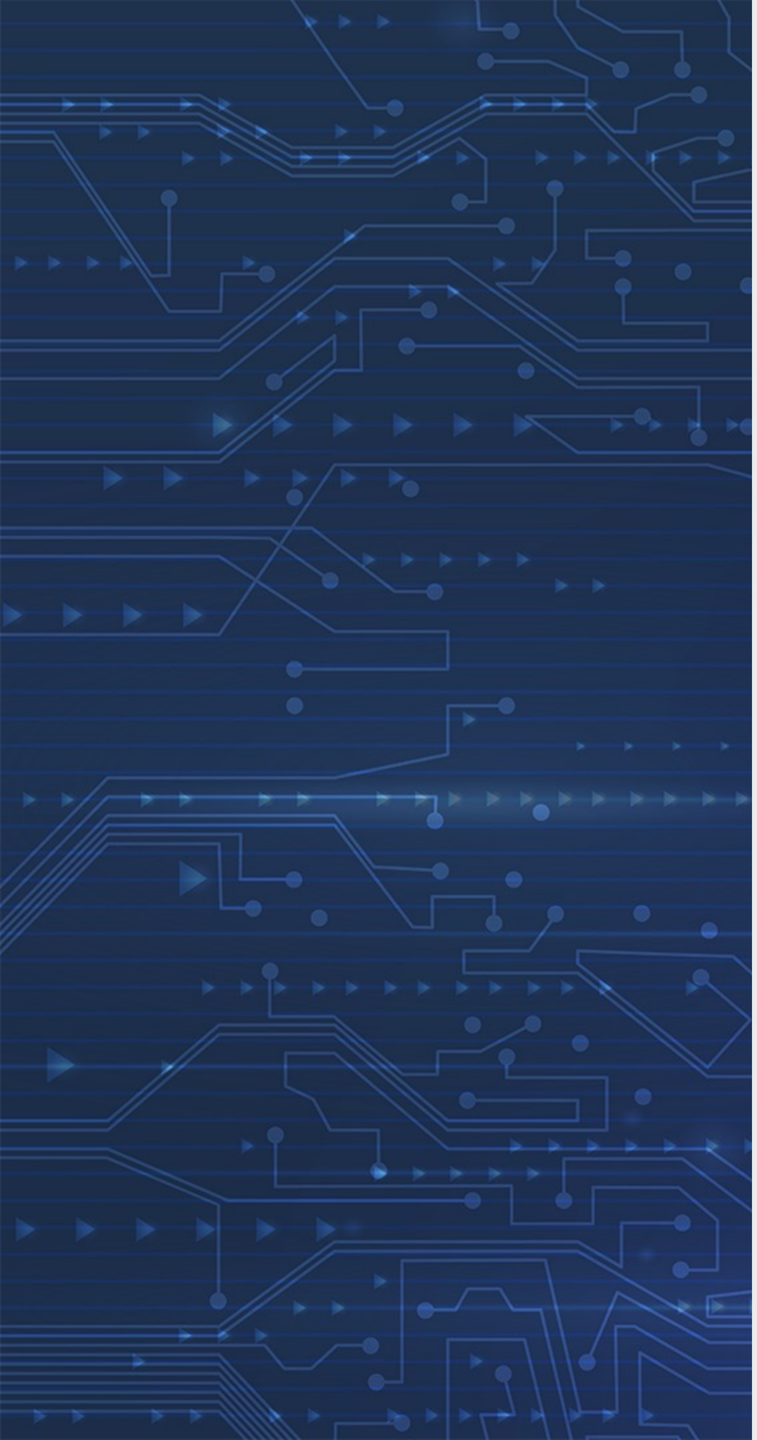
- This ZTA maturity model represents implementation of the Five Pillars through minor advancements made over achievable time periods.
- Per the Cybersecurity and Infrastructure Security Agency (CISA), “Each Pillar can progress at its own pace and may be farther along than others, until cross-pillar coordination is required.”

Zero Trust Drivers

- **Executive Order 14028:** Improving the Nation's Cybersecurity
  - Among other items, requires HHS to develop Zero Trust plan, adopt MFA, classify data, remove untrusted software, deploy EDR & manage devices, implement comprehensive log management
- **OMB M-21-31:** Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents
  - Establishes Federal-wide standards for cybersecurity logging and retention
- **OMB M-22-01:** Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response
  - Requires HHS to work with CISA on EDR rollout
- **OMB M-22-09:** Moving the U.S. Government Toward Zero Trust Cybersecurity Principles
  - Specific set of actions for each pillar of Zero Trust agencies must complete by the end of FY2024

Resources to Learn More

- CISA’s Zero Trust Maturity Model is a high-level overview of zero trust “pillars” that shows how agencies may progress to “Advanced” and “Optimal” states and describes how CISA service-offerings align to these pillars.
- CISA’s Cloud Security Technical Reference Architecture**,** co-authored with the United States Digital Service and FedRAMP, provides a more granular reference for secure cloud architectures and migration strategies. Available at:
- NIST’s SP 800-207, Zero Trust Architecture provides a consensus definition and framework for the key tenets of zero trust architecture, while describing several different approaches to zero trust architecture that organizations with different risk postures and skillsets can adopt.
- The NIST National Cybersecurity Center of Excellence (NCCoE) has initiated Implementing a Zero Trust Architecture, a collaboration with industry partners to apply the concepts in NIST SP 800-207 to a conventional enterprise architecture.
- GSA’s Zero Trust Architecture Buyer’s Guide can help agencies identify GSA contract vehicles that offer products and services relevant to agency zero trust implementations.
- The Department of Defense’s Zero Trust Reference Architecture comprehensively describes potential security features and architectural controls that the Department plans to execute across its systems.



What is HHS Doing?

Zero Trust Plan Requirements (M-22-09)

	ZERO TRUST PILLARS				
	IDENTITY	DEVICES	NETWORK	APPLICATIONS	DATA
OMB VISION	Federal staff have enterprise-managed accounts, allowing them to access everything they need to do their job while remaining reliably protected from even targeted, sophisticated phishing attacks	The devices that Federal staff use to do their jobs are consistently tracked and monitored, and the security posture of those devices is taken into account when granting access to internal resources	Agency systems are isolated from each other, and the network traffic flowing between and within them is reliably encrypted	Enterprise applications are tested internally and externally and can be made available to staff securely over the internet	Federal security teams and data teams work together to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information
REQUIREMENTS	Employ a centralized identity management system Require use of phishing resistant access methods	Employ user context along with identity to provide access Create a reliable, on-going, and complete inventory of IT assets	Complete and wide use of encryption for all network communications Monitor and restrict the use of none .GOV domains Develop a Zero Trust plan to isolate applications and environments	Fund and operate application security testing programs Utilize firms specializing in application security for independent third-party evaluation	Implement initial automation of data categorization managing access to sensitive documents Audit access to HHS data encrypted in commercial clouds Implement comprehensive logging and information sharing capabilities with CISA

HHS Activities & Challenges

	ZERO TRUST PILLARS				
	IDENTITY	DEVICES	NETWORK	APPLICATIONS	DATA
ACTIVITIES	Continued maturation of agency ICAM capabilities, consistent with OMB Memorandum M-19-17. This includes, but is not limited to, identity management programs, credential management services, multifactor authentication, and physical access control systems.	HHS' EDR deployment is currently being driven through the DHS program, but enhancements to the efforts currently outside of the DHS scope are necessary to fully implement visibility across cloud workloads and to enhance threat analytic capabilities.	Expand the deployment of Zero Trust and TIC 3.0 compliant solutions for VPN replacement, cloud access, and simplified networking to global field sites. Rearchitect internal networks and expedite move to cloud-based architectures	HHS has had significant success with the use of crowdsourced penetration testing for the deployment of vulnerability disclosure policy as well as securing of high-value assets and health informatics infrastructure.	Expedited planning and piloting of the HHS cloud-log aggregation capability which build on the existing Splunk-based log visibility platform at CSIRC. Data cataloging and data loss prevention capabilities are in place in some OpDivs.
BARRIERS	Expanding multi-factor authentication across all-systems and all environments overturns our risk-based approach and will significantly increase costs.	EDR deployment is currently being driven through the DHS program, but enhancements to the efforts currently outside of the DHS scope are necessary to fully implement visibility across cloud workloads and to enhance threat analytic capabilities Additional support needed to integrate EDR with cloud access solutions.	HHS has a large number of freezers, lab equipment, printers, and other network attached devices that do not support required technologies and will take longer than 180 days to retrofit.	Software development is a programmatic exercise and security capabilities are often required by contract, but standardization and oversite varies.	Expand implementation of data at rest encryption for legacy storage requires additional funding and resources. Protecting sensitive data on biomedical devices without impacting healthcare services.

HHS Zero Trust Working Group

- The purpose of the HHS Zero Trust Working Group is to provide a collaborative forum within which HHS and its Operating (OpDiv) and Staff (StaffDiv) Divisions can:
    - Refine and document HHS' Zero Trust Guiding Principles
    - Define roles and responsibilities of HHS and its OpDivs and StaffDivs
    - Track and share Division-level ZTA strategies and implementation plans
    - Identify Anchor Projects to leverage lessons learned and applicability for an HHS-wide approach
    - Guide the development of Zero Trust related polices and standards
    - Identify and recommend enterprise procurement strategies
- Convening bi-weekly since 11/17/2022, the working group has benefited from a high degree of engagement and collaboration. Participants have provided responses to data calls around current Zero Trust Architecture status and enabled HHS to response to the Federal CIO regarding implementation of action items described in M-22-09.
- The group has also worked to prepare for the request and execution of the FY23 Zero Trust NEF Budget and planning for FY24 priorities.

HHS Zero Trust Status Survey (12/2022)

Challenges

- Removal of Password Policies ✓
- Phishing-resistant MFA
- Comprehensive Logging
- Migration of FISMA Moderate System ✓
- Data Categorization ✓

How confident are you that your entire organization can meet this goal and timeframe?

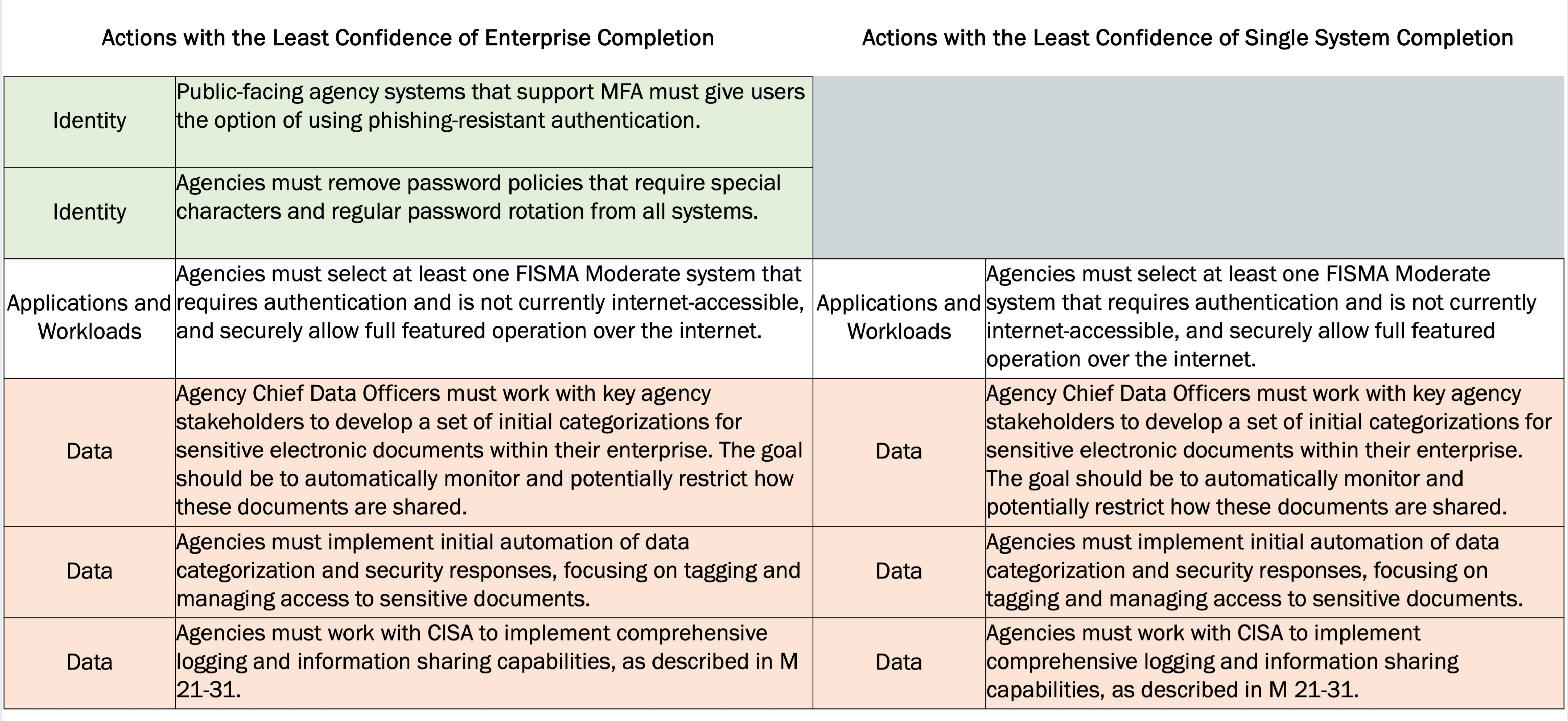
	No Answer	Not At All	Slightly \ Moderately	Very \ Extremely
Identity	18%	18%	27%	36%
Device	21%	9%	24%	45%
Network	18%	0%	48%	34%
Application & Workload	18%	13%	30%	39%
Data	18%	20%	52%	9%

How confident are you that one or more of your systems can meet this goal and timeframe?

	No Answer	Not At All	Slightly \ Moderately	Very \ Extremely
Identity	18%	9%	20%	53%
Device	21%	9%	15%	55%
Network	18%	0%	36%	45%
Application & Workload	18%	8%	27%	47%
Data	18%	14%	48%	20%

Office of
Information Security
Securing One HHS

HHS Zero Trust Survey Results (12/2022)



Actions with the Least Confidence of Enterprise Completion		Actions with the Least Confidence of Single System Completion	
Identity	Public-facing agency systems that support MFA must give users the option of using phishing-resistant authentication.		
Identity	Agencies must remove password policies that require special characters and regular password rotation from all systems.		
Applications and Workloads	Agencies must select at least one FISMA Moderate system that requires authentication and is not currently internet-accessible, and securely allow full featured operation over the internet.	Applications and Workloads	Agencies must select at least one FISMA Moderate system that requires authentication and is not currently internet-accessible, and securely allow full featured operation over the internet.
Data	Agency Chief Data Officers must work with key agency stakeholders to develop a set of initial categorizations for sensitive electronic documents within their enterprise. The goal should be to automatically monitor and potentially restrict how these documents are shared.	Data	Agency Chief Data Officers must work with key agency stakeholders to develop a set of initial categorizations for sensitive electronic documents within their enterprise. The goal should be to automatically monitor and potentially restrict how these documents are shared.
Data	Agencies must implement initial automation of data categorization and security responses, focusing on tagging and managing access to sensitive documents.	Data	Agencies must implement initial automation of data categorization and security responses, focusing on tagging and managing access to sensitive documents.
Data	Agencies must work with CISA to implement comprehensive logging and information sharing capabilities, as described in M 21-31.	Data	Agencies must work with CISA to implement comprehensive logging and information sharing capabilities, as described in M 21-31.

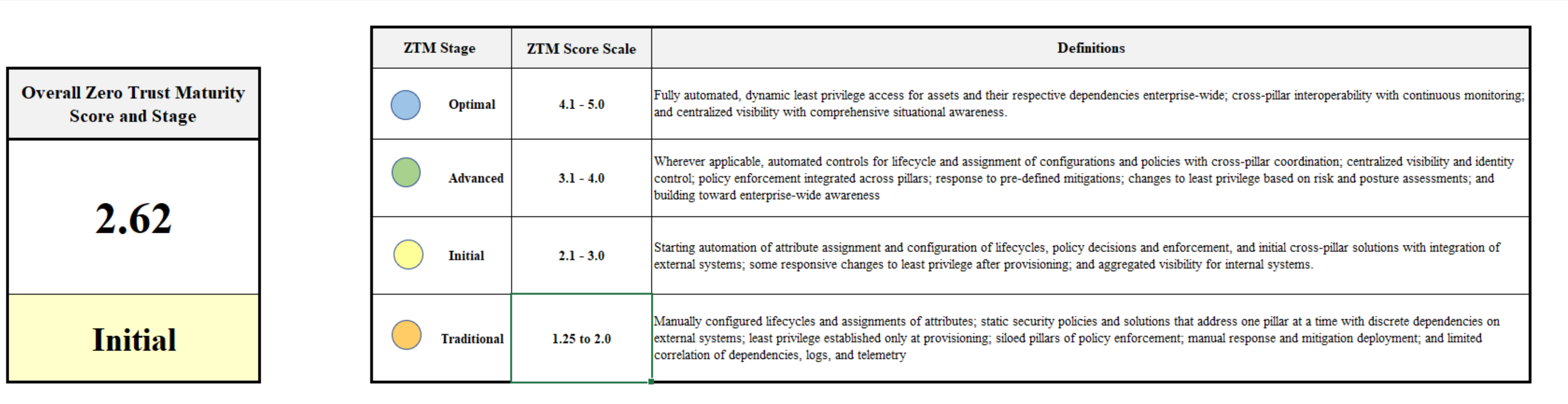
HHS Zero Trust Maturity Scorecard

- Following the guidance provided by CISA's Zero Trust Maturity Model (version 2.0) HHS OCIO has developed an assessment and proposed methodology to create and maintain the HHS Zero Trust Maturity Scorecard.
- Goals for the scorecard include:
  - Define the current maturity stage in each FISMA system
  - Identify gaps for Zero Trust implementation
  - Designate the next planned actions for Zero Trust implementation
  - Describe budget allocations and execution timelines

CISA's ZTMM Pillar	Total Number of Questions
Identity	7
Devices	7
Networks	7
Applications and Workloads	8
Data	8
Cross-Cutting Capabilities	3
TOTAL	40

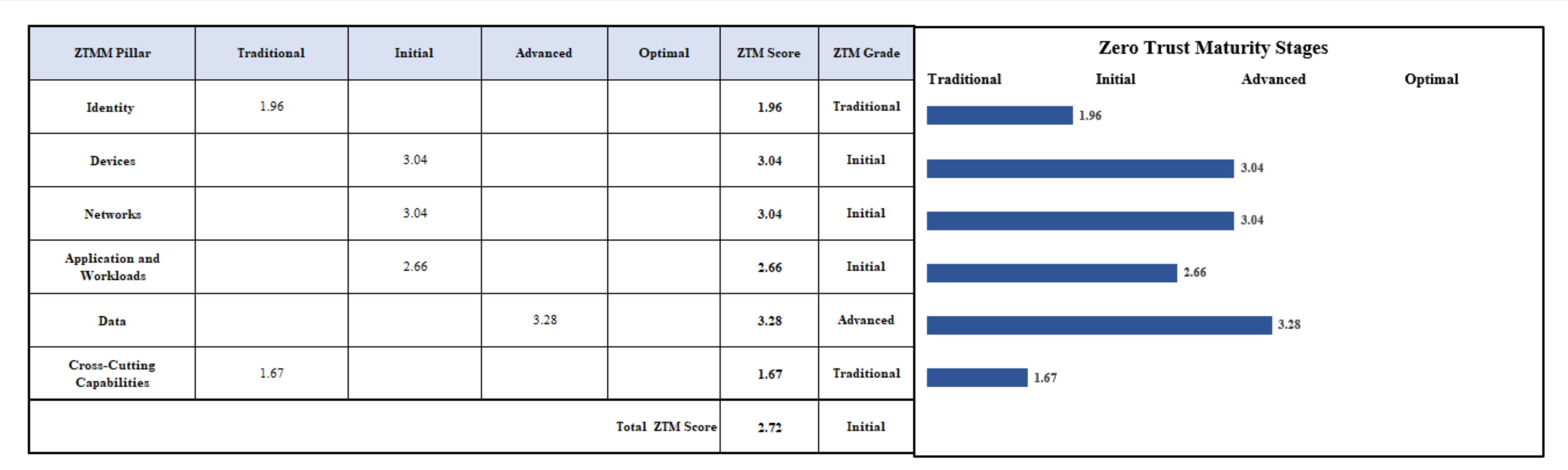
HHS Zero Trust Maturity Scorecard

Sample Dashboard System X (Grading Scheme: Score/Maturity Stage)



Overall Zero Trust Maturity Score and Stage
2.62
Initial

ZTM Stage	ZTM Score Scale	Definitions
🔵 Optimal	4.1 - 5.0	Fully automated, dynamic least privilege access for assets and their respective dependencies enterprise-wide; cross-pillar interoperability with continuous monitoring; and centralized visibility with comprehensive situational awareness.
🟢 Advanced	3.1 - 4.0	Wherever applicable, automated controls for lifecycle and assignment of configurations and policies with cross-pillar coordination; centralized visibility and identity control; policy enforcement integrated across pillars; response to pre-defined mitigations; changes to least privilege based on risk and posture assessments; and building toward enterprise-wide awareness
🟡 Initial	2.1 - 3.0	Starting automation of attribute assignment and configuration of lifecycles, policy decisions and enforcement, and initial cross-pillar solutions with integration of external systems; some responsive changes to least privilege after provisioning; and aggregated visibility for internal systems.
🟠 Traditional	1.25 to 2.0	Manually configured lifecycles and assignments of attributes; static security policies and solutions that address one pillar at a time with discrete dependencies on external systems; least privilege established only at provisioning; siloed pillars of policy enforcement; manual response and mitigation deployment; and limited correlation of dependencies, logs, and telemetry



ZTMM Pillar	Traditional	Initial	Advanced	Optimal	ZTM Score	ZTM Grade
Identity	1.96				1.96	Traditional
Devices		3.04			3.04	Initial
Networks		3.04			3.04	Initial
Application and Workloads		2.66			2.66	Initial
Data			3.28		3.28	Advanced
Cross-Cutting Capabilities	1.67				1.67	Traditional
				Total ZTM Score	2.72	Initial

Zero Trust Maturity Stages

Scoring Explained

Multiply the sum of each pillar by 5 and divide by the maximum score to produce the ZTM score.

Identity, Devices, and Networks:

- There are 7 questions and 4 choices (1 to 4). The minimum score is 7 (if all answers are #1) and the maximum is 28 (if all answers are #4)
  - If the total score for Identity = 7, then the ZTM scale (7*5)/28 = 1.25
  - If the total score for Identity = 28, then the ZTM scale (28*5)/28 = 5

Application & Data:

- There are 8 questions for these sections, so the same equation applies, but divide by 32.

Cross Cutting Capabilities:

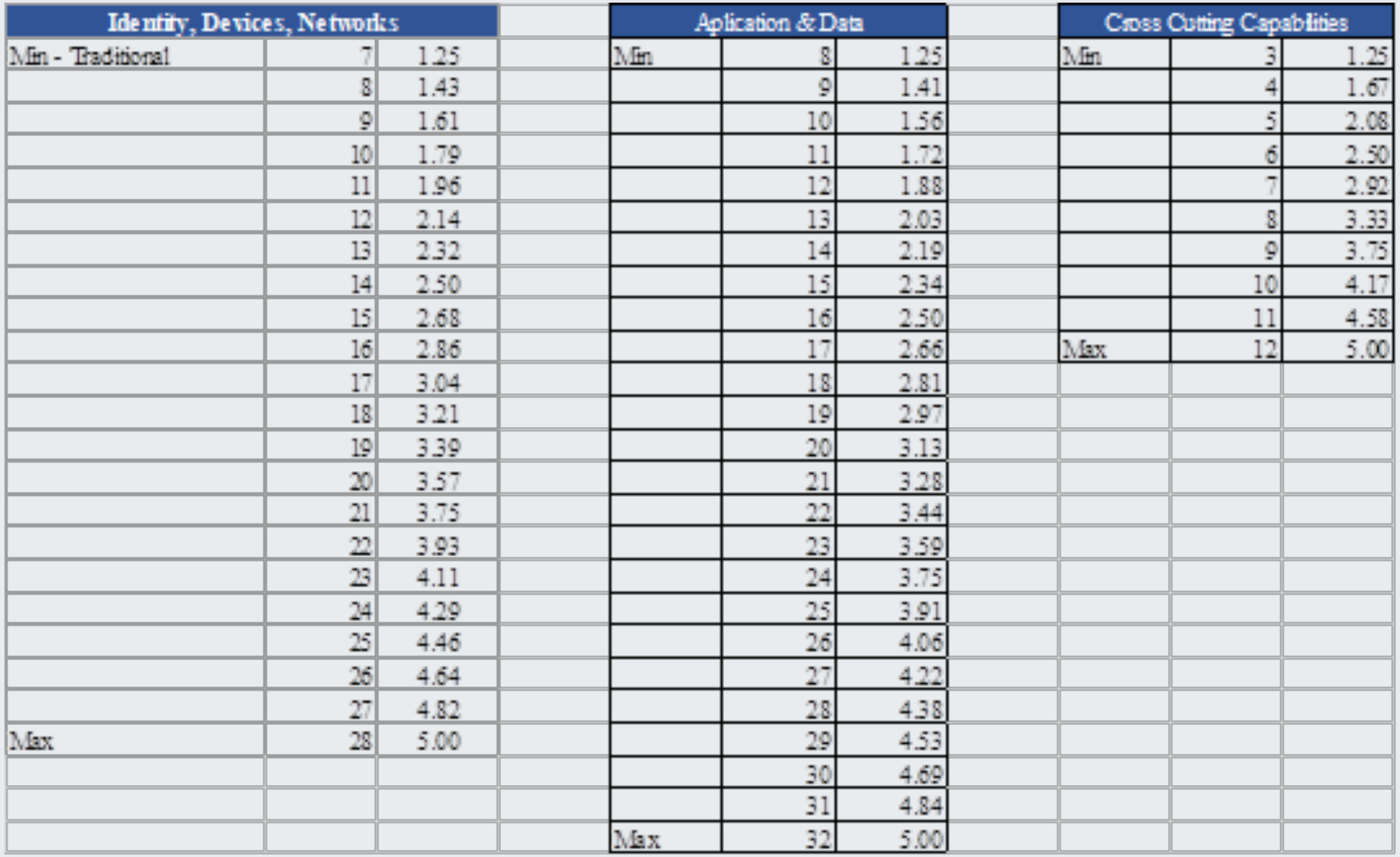
- There are 3 questions for this section, so the same equation applies, but divide by 12.

Total Scorecard

- There are 40 questions in the scorecard, so the same equation applies, but divide by 160.

Scoring Tables

Note this is not a grade to be scrutinized, but an assessment of present status.



Identity, Devices, Networks		
Min - Traditional	7	1.25
	8	1.43
	9	1.61
	10	1.79
	11	1.96
	12	2.14
	13	2.32
	14	2.50
	15	2.68
	16	2.86
	17	3.04
	18	3.21
	19	3.39
	20	3.57
	21	3.75
	22	3.93
	23	4.11
	24	4.29
	25	4.46
	26	4.64
	27	4.82
Max	28	5.00

Aplication & Data		
Min	8	1.25
	9	1.41
	10	1.56
	11	1.72
	12	1.88
	13	2.03
	14	2.19
	15	2.34
	16	2.50
	17	2.66
	18	2.81
	19	2.97
	20	3.13
	21	3.28
	22	3.44
	23	3.59
	24	3.75
	25	3.91
	26	4.06
	27	4.22
	28	4.38
	29	4.53
	30	4.69
	31	4.84
Max	32	5.00

Cross Cutting Capablities		
Min	3	1.25
	4	1.67
	5	2.08
	6	2.50
	7	2.92
	8	3.33
	9	3.75
	10	4.17
	11	4.58
Max	12	5.00

TIPS & Tech Exchanges

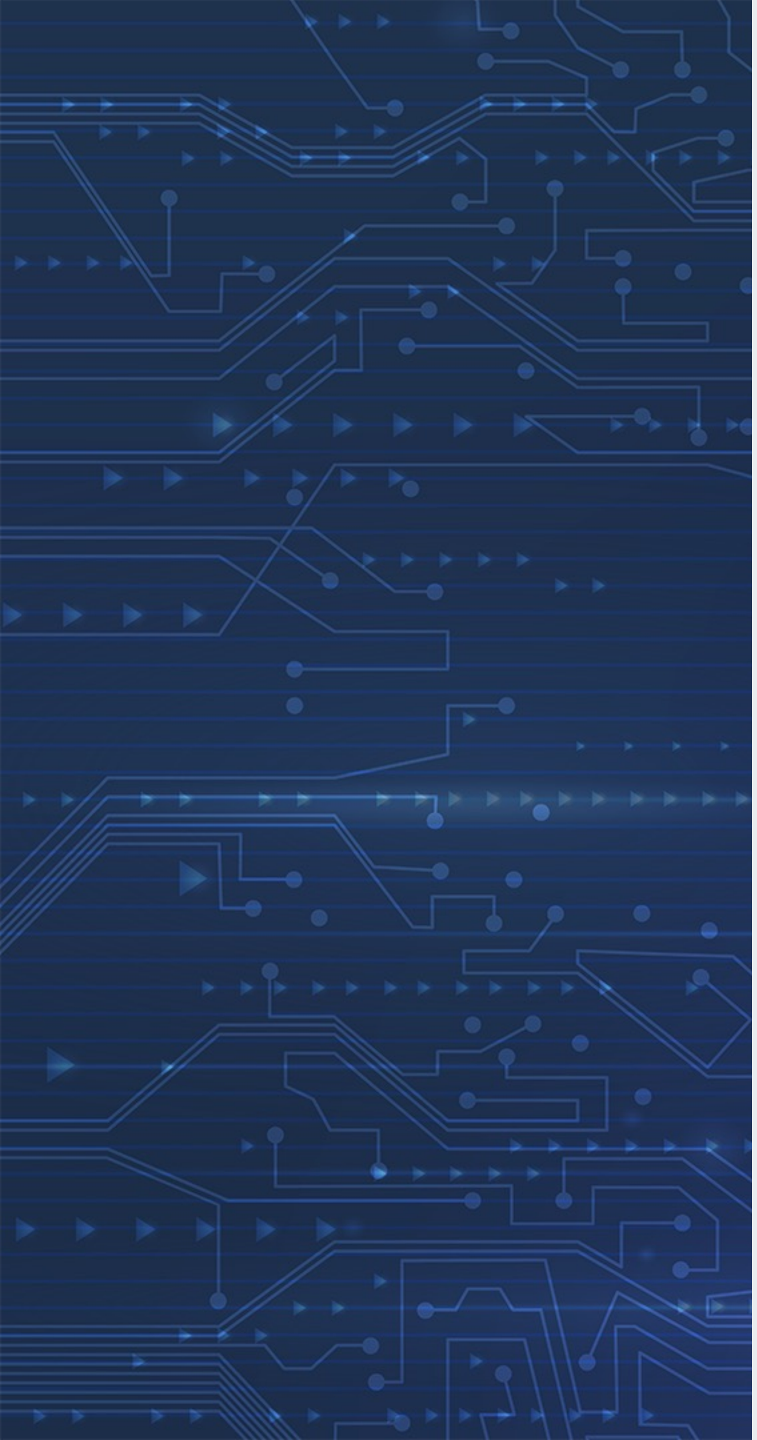
Technology Innovation & Product Sessions (TIPS) allow participants to connect directly with vendors about how products would operate in their environments.

Wednesdays 11-11:45am ET

HHS Tech Exchanges highlight specific deployments and integrations that are helpful to share across the Department. These events are presented by and for HHS employees, with support from relevant vendors, and are open to all HHS employees and contractors.

Contact sdi@hhs.gov to be added to our distribution list! CPE credits available.

Questions



M-23-02 – Migrating to Post Quantum Cryptography

Speaker: Conrad Bovell

Key Terms

Term	Definition
Cryptanalytically Relevant Quantum Computer (CRQC)	A computer capable of undermining current public-key cryptographic algorithms.
Quantum Computer	A computer utilizing the collective properties of quantum states, such as superposition, interference and entanglement, to perform calculations. These computers can solve a subset of hard mathematical problems at a much faster rate than a classical (i.e., nonquantum) computer.
Cryptographic Agility	A design feature that enables future updates to cryptographic algorithms and standards without the need to modify or replace the surrounding infrastructure.
Cryptographic System	An active software or hardware implementation of one or more cryptographic algorithms that provide one or more of the following services: creation and exchange of encryption keys, encrypted connections, or creation and validation of digital signatures.

M-23-02 Purpose

- OMB, in coordination with the Office of National Cyber Director (ONCD), issued M-23-02, Migrating to Post Quantum Cryptography, on November 18, 2022.
  - M-23-02 describes preparatory steps for agencies to undertake as they begin their transition to PQC by conducting a prioritized inventory of cryptographic systems.
  - The memorandum provides transitional guidance to agencies in the period before PQC standards are finalized by the National Institute of Standards and Technology (NIST), after which OMB will issue further guidance.

M-23-02: Migrating to Post Quantum Cryptography (PQC) & Agency Actions

- **November 18, 2022:** OMB released M-23-02: Migrating to Post-Quantum Cryptography.
- The threat posed by the prospect of a cryptanalytically relevant quantum computer (CRQC) requires that agencies prepare now to implement post-quantum cryptography (PQC)
- Once operational, a CRQC is expected to be able to compromise certain widely used cryptographic algorithms used to secure Federal data and information systems.

<u>Agency Actions Completed:</u>

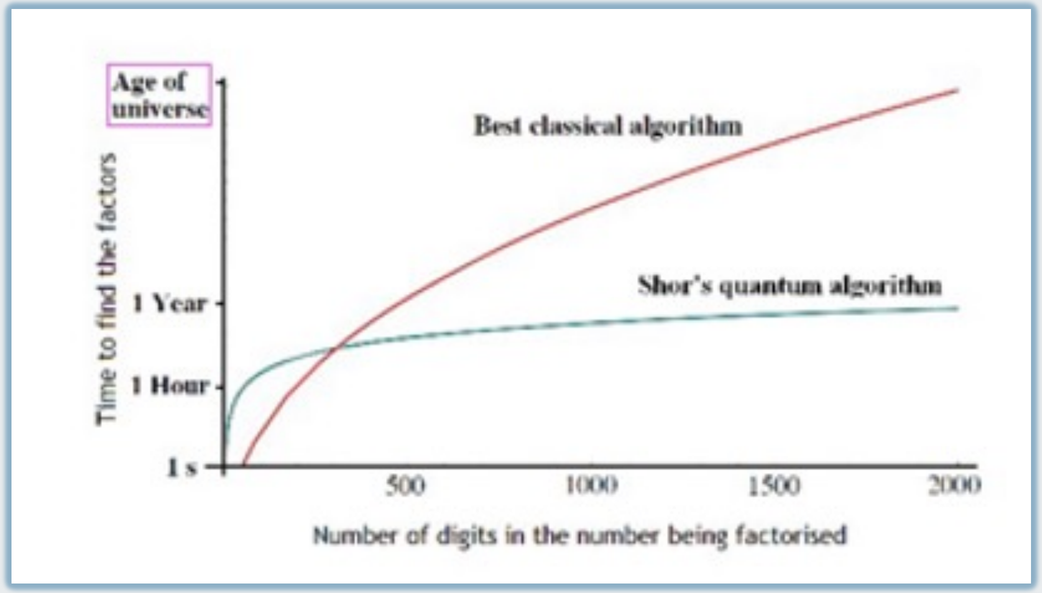
- **December 18, 2022**: Designate cryptographic inventory and migration lead
  - HHS - Conrad Bovell
- **May 4, 2023**: Submit cryptographic system inventory and annually thereafter until 2035
  - Initial focus is on High Value Assets (HVAs) and high impact systems whether operated by the agency or on the agency's behalf
  - OMB expects to direct inventory of other vulnerable agency systems or assets, not in the above scope, through future guidance on Federal Information System Modernization Act (FISMA) of 201412
- **June 4, 2023**: Submit funding assessments and annually thereafter

The Availability of Quantum Computers

- Small QCs are available today for use in limited types of applications, but CRQCs are not available yet.
  - Several QC cloud platforms are available, including Google, IBM, Microsoft, and Amazon.
  - Commercial companies, such as Volkswagen and Goldman Sachs, are using QCs in their day-to-day operations for specific tasks.
  - Today's largest QCs have hundreds of qubits. IBM's roadmap extrapolates development of a one million-qubit computer by 2030.
- **Theoretically, with today's technology, Shor's Algorithm will require a quantum computer with roughly eight million qubits to break RSA-1024 or 2048.**
- The USG is using 2035 as a target transition date to PQC as stated in NSM-10.
- To be fair, a CRQC requires much more than just number of qubits; however, based on previous cryptographic transitions we are not moving too early.

The Impact to Cryptography

- Shor’s Algorithm for factoring prime numbers with a QC is the current known threat
- It represents an exponential reduction in time for some forms of decryption but mostly for cryptanalysis
  - Decryption is used as an authorized key to revert to plain text and that time is unaffected
- Implies that current public key cryptography can be broken in an unacceptable timeframe



NIST is working to standardize PQC algorithms to render Shor’s Algorithm ineffective (in the future). New PQC algorithms are not affected by Shor’s factoring capability.

List of CRQC-Vulnerable Algorithms

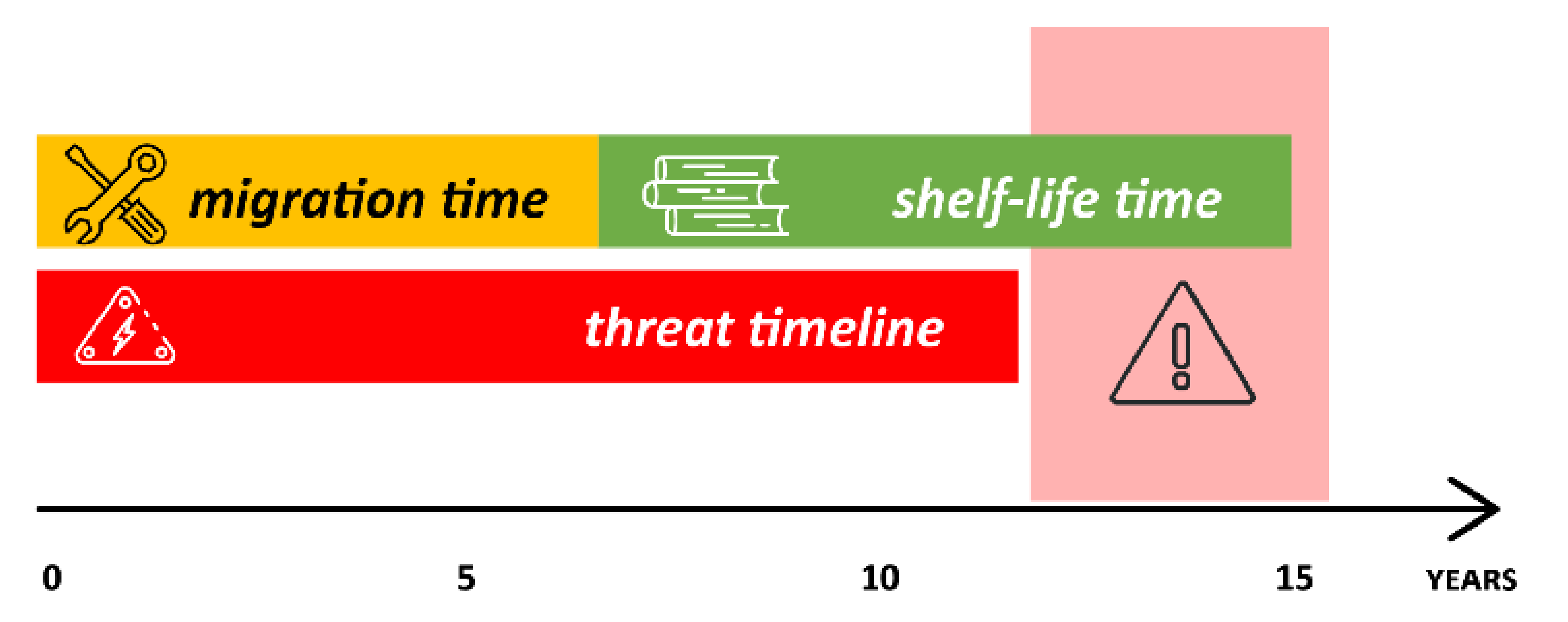
NIST & OMB will publish guidance which will emphasize a focus exclusively on Asymmetric Algorithms. Symmetric algorithms are not susceptible to Shor's algorithm.

Algorithm	Function	Specification
Elliptic Curve Diffie-Hellman (ECDH) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A/B/C
Menezes-Qu-Vanstone (MQV) Key Exchange	Asymmetric algorithm used for key establishment	NIST SP 800-56A/B/C
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithms used for digital signatures	FIPS PUB 186-4
Diffie-Hellman (DH) Key Exchange	Asymmetric algorithm used for key establishment	IETF RFC 3526
RSA Signature Algorithm	Asymmetric algorithm used for key establishment	FIPS SP 800-56B Rev. 1
Digital Signature Algorithm (DSA)	Asymmetric algorithm used for digital signatures	FIPS PUB 186-4
Other non-PQC Asymmetric Algorithm[19]	Remaining asymmetric algorithms not enumerated in the list above	Not applicable

M-23-02 Inventory Prioritization

- The inventory must encompass each information system or asset that is **any** of the following, whether operated by the agency or on the agency's behalf: A high impact information system;
- An agency **High Value Asset (HVA);** or
  - Any other system that an agency determines is likely to be particularly vulnerable to CRQC-based attacks. Agencies should include information systems or assets that: **Contain data expected to remain mission-sensitive in 2035**; or
  - Are **logical access control systems based in asymmetric encryption** (such as a **Public Key Infrastructure**) that use any of the algorithms listed in Appendix B withinM-23-02.

Quantum Threat Risk Determination



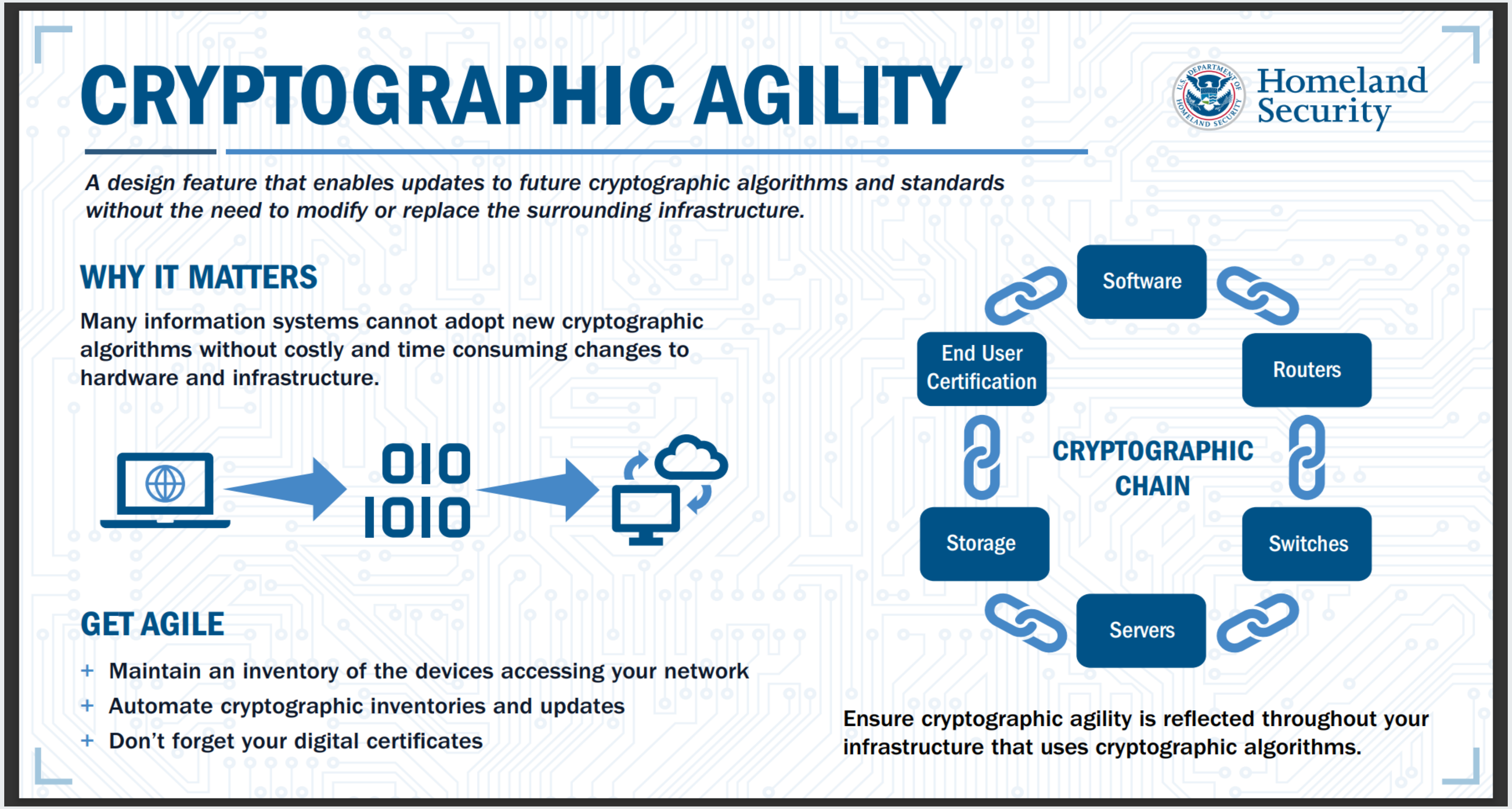
HHS Approach in Developing Initial Response

- Engage NIST National Cybersecurity Center of Excellence (NCCoE) on their efforts to develop solutions as part of their “Migration to Post-Quantum Cryptography Project” which entails the NCCoE working with the private sector to address cybersecurity challenges posed by the transition to quantum-resistant cryptography.
  - This project shall develop programs for discovery and remediation of any system that does not use quantum –resistant cryptography or that remains dependent on vulnerable systems.
  - NCCoE Engineering lead briefed HHS CISO Council meeting on details of NIST’s efforts
  - HHS hosting **Quantum Technology Innovation & Product Sessions (Q-TIPS)** where NCCoE collaborating vendors brief FCEB orgs.
- Engage CISA on their approach to support agencies in their efforts to address challenges associated with meeting initial PQC migration requirements.
  - As a result of HHS’ engagement, CISA invited HHS to provide an overview of their efforts during the Agency Spotlight section of their CyberStat Workshop titled “Migrating to Post Quantum Cryptography: Implementation of NSM 10” held on March 28, 2023.
  - HHS provided briefing on intersection of M-23-02 and ZTMM 2.0 July 21st Quarterly meeting of CISA Federal Zero Trust Managers CoP
- Engage OMB to hear their prospective on initial requirements and responses to the many questions that exist.
- Engage GSA to positively impact acquisition of products that can support Cryptographic Agility

HHS Agency Spotlight:
March 2023 PQC Migration CyberStat Workshop

- Leverage automated aolutions NCCoE is developing
  - Review the list of NCCoE collaborating vendors
  - HHS Administration for Strategic Preparedness and Response (ASPR) leveraged solution developed by NCCoE vendor to conduct cryptographic inventory
  - Solutions have been developed that can leverage EDR solutions to conduct cryptographic inventories
  - Leverage NCCoE developed solutions to achieve Cryptographic Agility and support Zero Trust continuous monitoring requirements
  - Incorporate PQC migration into agency Zero Trust planning, noting its impact to all five pillars

Cryptographic Agility



CRYPTOGRAPHIC AGILITY

Homeland Security

A design feature that enables updates to future cryptographic algorithms and standards without the need to modify or replace the surrounding infrastructure.

WHY IT MATTERS

Many information systems cannot adopt new cryptographic algorithms without costly and time consuming changes to hardware and infrastructure.

GET AGILE

- Maintain an inventory of the devices accessing your network
- Automate cryptographic inventories and updates
- Don't forget your digital certificates

CRYPTOGRAPHIC CHAIN

Software

Routers

Switches

Servers

Storage

End User Certification

Ensure cryptographic agility is reflected throughout your infrastructure that uses cryptographic algorithms.

CISA Zero Trust Maturity Model 2.0 Data Pillar

Published April 2023

Function	Traditional	Initial	Advanced	Optimal
Data Encryption	Agency encrypts minimal agency data at rest and in transit and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency encrypts all data in transit and, where feasible, data at rest (e.g., mission critical data and data stored in external environments) and begins to formalize key management policies and secure encryption keys	Agency encrypts all data at rest and in transit across the enterprise to the maximum extent possible, begins to incorporate cryptographic agility, and protects encryption keys (i.e., secrets are not hard coded and are rotated on a regular basis).	Agency encrypts data in use where appropriate, enforces least privilege principles for secure key management enterprise-wide, and applies encryption using up-to-date standards and cryptographic agility to the extent possible.

CISA Zero Trust Maturity Model 2.0 Network Pillar

Published April 2023

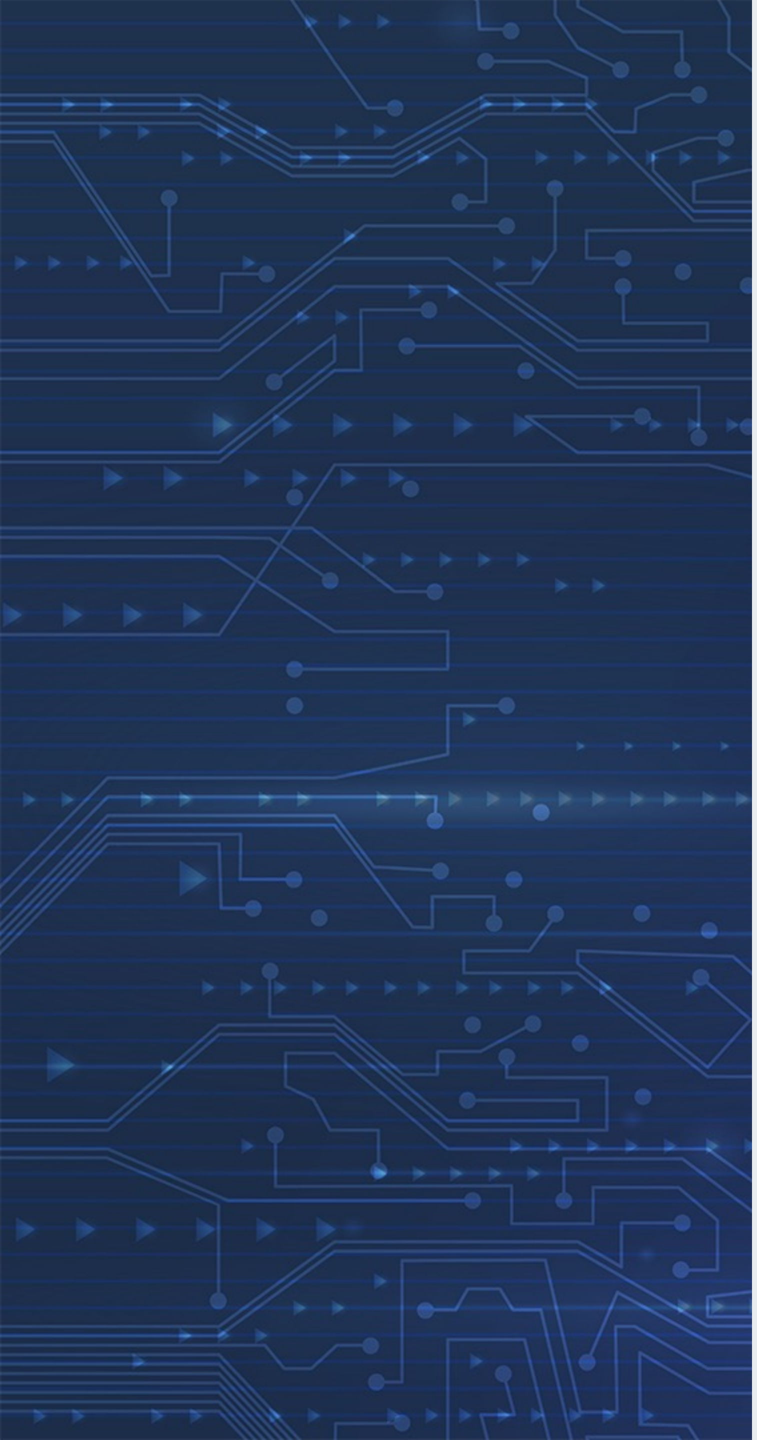
Function	Traditional	Initial	Advanced	Optimal
Traffic Encryption (Formerly Encryption)	Agency encrypts minimal traffic and relies on manual or ad hoc processes to manage and secure encryption keys.	Agency begins to encrypt all traffic to internal applications, to prefer encryption for traffic to external applications [27], to formalize key management policies, and to secure server/service encryption keys	Agency ensures encryption for all applicable internal and external traffic protocols,[28] manages issuance and rotation of keys and certificates, and begins to incorporate best practices for cryptographic agility.[29]	Agency continues to encrypt traffic as appropriate, enforces least privilege principles for secure key management enterprise wide, and incorporates best practices for cryptographic agility as widely as possible.

[27] For example, when both HTTP and HTTPS options are available, policies and settings prefer HTTPS.

[28] There are a variety of resources agencies should review in regard to encrypting and decrypting network traffic (or not) for inspection and visibility needs as part of their zero trust adoption: OMB M-15-13, M-19-26, M-22-09, DHS Binding Operational Directive 18-01, NIST SP 800-207, among others. See also: https://www.cisa.gov/uscert/ncas/alerts/TA17-075A.

[29] DHS. Cryptographic Agility Infographic. May 12, 2022. https://www.dhs.gov/publication/cryptographic-agility-infographic

? Questions



Embracing Rapid Cybersecurity Advancements to Defend Health Networks

Speaker: Rahul Gaitonde

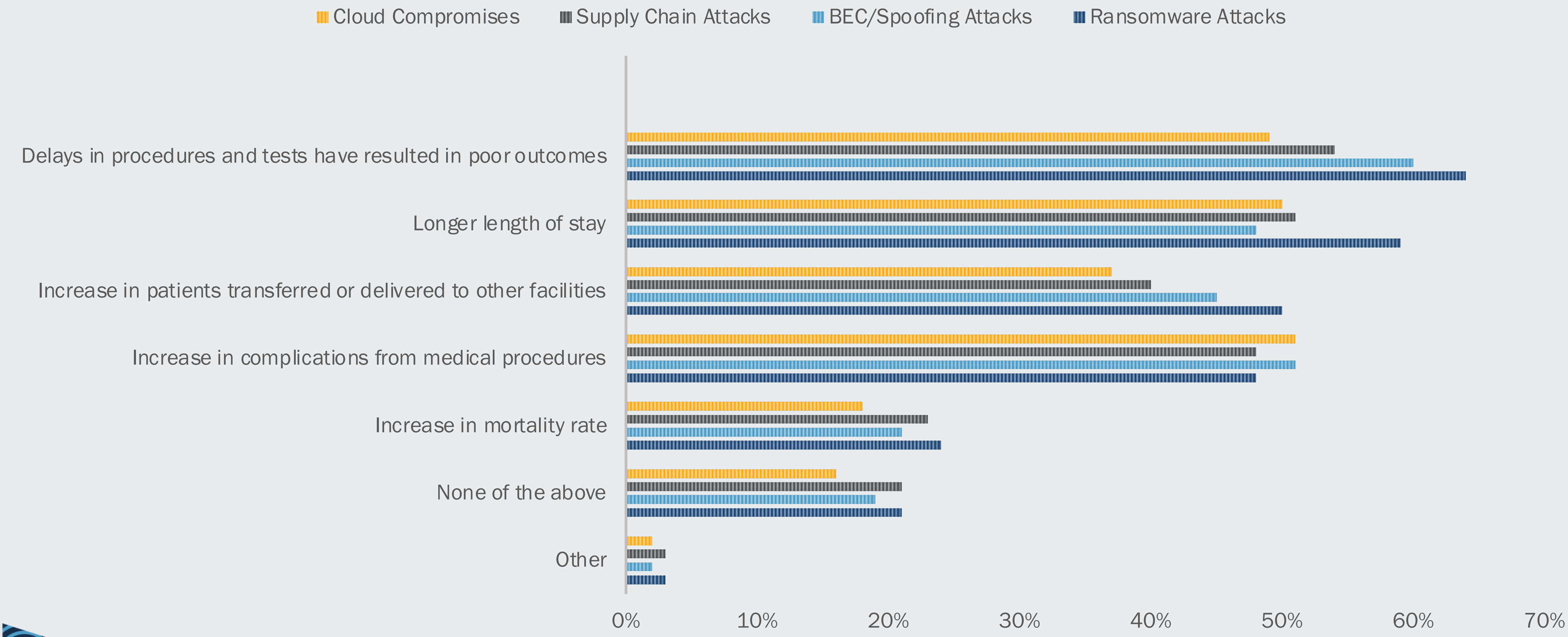
HC3 History & Mission

- The **Health Sector Cybersecurity Coordination Center (HC3)** was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats, as well as for sundry other purposes.
- HC3's mission is to support the defense of the Healthcare and Public Health (HPH) sector's information technology infrastructure, by strengthening coordination and information sharing within the sector and by cultivating cybersecurity resilience, regardless of organizations' technical capacity.
- HC3 provides objective information to the Healthcare and Public Health (HPH) sector.

The Health Sector Continues to Be a Primary Target

- In 2022, HPH entities in the United States suffered an average of 1,410 weekly cyberattacks per organization, resulting in an 86% increase in attacks compared to 2021.
- The HPH sector now ranks second out of all critical infrastructure sectors for the most cyberattacks in the country.
- In 2023, IBM Security's Annual Cost of a Data Breach Report found that the average price tag of a healthcare data breach had climbed to $11 million.
- Cyberattacks on the healthcare industry yield higher profits for criminals, as health information can fetch about $1,000 per record on the dark web (compared to about $5 per credit card number and $1 per social security number).

Impact of a Cyber Attack on Patient Care



Office of
Information Security
Securing One HHS

Cloud Computing

- According to a report by Precedence Research, the global healthcare cloud computing market size was valued at USD 30.5 billion in 2021 and is predicted to surpass around USD 127.04 billion by 2030.
- Embracing the cloud has allowed the health sector to see massive gains in efficiency and scalability.
- The cloud poses many unique security threats, including:
  - Insecure interfaces, such as APIs and Third-Party Resources
  - Insufficient identity, credential, access and key management (ICAM)
  - Misconfiguration and exploitation of serverless and container workloads
- Key mitigations include:
  - **Use a cloud security posture management (CSPM) solution:** CSPM solutions can help organizations to identify and remediate security vulnerabilities in their cloud environment, including insecure interfaces and APIs.
  - **Use a zero-trust security model:** This model assumes that no user or device is trusted by default and requires them to authenticate themselves and their devices before they are granted access to resources.
  - **Use a cloud infrastructure entitlement management (CIEM) solution:** A CIEM solution can help organizations to track and manage user and entity access to cloud resources, including serverless and container workloads.

Social Engineering Attacks

- Social engineering is the manipulation of human psychology for one's own gain. A social engineer can manipulate staff members into giving the threat actor access to various systems.
- Carahsoft's 2021 HIMSS Healthcare Cybersecurity Survey: Over a 12-month period, phishing attacks were the most common threat, accounting for 45% of security incidents, followed by ransomware.
- AI is now being used to develop Phishing, Business Email Compromise, and Callback Phishing.
- Mitigations:
    - **Monitor for suspicious activity:** Organizations should monitor their network for suspicious activity, such as unusual login attempts or data exfiltration.
    - **Enable MFA:** The victim will also need to provide a second factor of authentication, such as a code from their security token or a fingerprint, in order to log in. This makes it much more difficult for the attacker to steal the victim's password.
    - **Enable Zero Trust:** In a zero-trust model, the attacker will also need to spoof the authentication server. This is much more difficult to do, and it can help to prevent the attacker from gaining access to the account.

Internet of Things (IoT)

- Hospitals and healthcare facilities use dozens—if not hundreds—of IoT devices, including wearable medical devices, guided imagery, monitoring sensors, implants, etc. These devices allow healthcare professionals to assist and monitor patients remotely for convenient and cost-effective services.
- According to a recent report by BusinessWire, 57% of healthcare organizations do not always change default usernames and passwords for devices, and 82% run connected devices on legacy systems.
- Key mitigations:
  - **Use a secure network:** IoT devices should be connected to a secure network that is protected by firewalls and other security measures.
  - **Keep IoT devices up to date:** IoT devices often have software vulnerabilities that can be exploited by attackers. It is important to keep IoT devices up to date with the latest security patches.
  - **Whitelist devices:** Devices should be whitelisted to be added to the network, and non-approved devices should be automatically blocked.
  - **Change defaults:** All devices should have passwords and other configurations changed from the factory standard, and use role-based access if possible.

Emerging Technologies

5G

- 5G is approximately 10 to 100 times faster than typical current cellular connections, faster than residential physical fiber optic cable, and can handle a significantly greater number of devices simultaneously (IoT).
- Significantly reduced latency: 20 milliseconds to 1 millisecond.
- Robotics autonomously or semi-autonomously performing medical procedures.
- 5G is expected to make telesurgery possible due to the low latency that it offers, as well as its enhancements to robotics, which would then aid surgery.
- In the future, language translators will be able to video conference with the patient and doctor using models at the network edge with low latency.
- 5G technology enables IoT networks to operate in a stable, fast and highly reliable manner.
- Security concerns:
  - Need to secure medical devices as they connect to the network (authentication).
  - Need to secure data as it is transmitted to/from medical devices (end-to-end encryption).
  - Need to secure data on device (whole disk encryption or similar procedure).

Artificial Intelligence

- Benefits of AI to the health sector:
  - Analysis of big data sets
    - Accelerated clinical decisions
      - Example: Interpretation of medical imaging
    - Improved (deeper) patient insights → predictive analysis
      - Connecting disparate health data (integrated electronic health records)
    - New drug discovery and preventive medicine
  - Medical devices (Software-as-a-Medical-Device/SaMD)
    - "...software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device“
- Security concerns:
  - Artificial Intelligence requires the gathering of very large collections of data in order to learn.
  - Privacy and security concerns regarding protected health information (PHI).
  - U. California at Berkeley 2019 study: Artificial intelligence advances threaten privacy of health data
  - Therefore, data needs to be protected at rest and in motion:
    - Data repository security
    - End-to-end encryption and multi-factor authentication
  - Artificial intelligence allows for the re-identification of de-identified data

Nanomedicine

- What is nanomedicine?
  - One definition: “The comprehensive monitoring, control, construction, repair, defense, and improvement of human biological systems at the molecular level, using engineered nanodevices and nanostructures, operating massively in parallel at the single-cell level, performing ‘single-cell medicine,’ ultimately to achieve medical benefit.” (Schachat, 2018)
  - In simpler terms, it is the medical application of nanotechnology.
    - Very small technology; smaller than 100 nanometers (1 billion nanometers = 1 meter).
- Security concerns:
  - Remote connectivity
    - Ransomware and the disruption of nanotechnology devices with theoretically fatal consequences.
    - Compromise of many nanodevices for traffic flooding/DDoS.
  - Weaponized inhalable particles as a delivery system for bioterrorism.
  - Penetration and security testing is likely going to play a big role in securing nanomedicine technologies.

Quantum Computing and Cryptography

- Quantum computing is a type of computing that uses the principles of quantum mechanics to perform calculations. Quantum computers can solve certain types of problems that are intractable for classical computers, such as simulating the behavior of molecules, breaking encryption codes, and searching through large databases.
- Drug discovery: Quantum computers could be used to simulate the behavior of molecules, which could help scientists to develop new drugs more quickly and efficiently.
- Security concerns:
  - Many of the encryption standards that are used today, such as RSA and Diffie-Hellman, are based on mathematical problems that are believed to be difficult for classical computers to solve. However, quantum computers could be used to solve these problems much more quickly, which would make it possible for hackers to break these encryption standards.

Reference Materials

References

- “Top Healthcare Cybersecurity Predictions for next Year.” *HealthITSecurity*. https://healthitsecurity.com/features/top-healthcare-cybersecurity-predictions-for-next-year.
- “Cost of a Data Breach 2022.” IBM. 2022. https://www.ibm.com/reports/data-breach.
- “The State of Healthcare Cybersecurity: Top Insights and Trends.” n.d. Www.bitlyft.com. https://www.bitlyft.com/resources/state-healthcare-cybersecurity.
- “Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks.” Check Point Blog. January 5, 2023. https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/).
- https://www.proofpoint.com/us/cyber-insecurity-in-healthcare
- “Cyber Insecurity in Healthcare: Cost & Impact on Patient Care | Proofpoint US.” Proofpoint. July 26, 2022. https://www.proofpoint.com/us/cyber-insecurity-in-healthcare.
- “Healthcare Cloud Computing Market Size 2022-2030.” n.d. Www.precedenceresearch.com. https://www.precedenceresearch.com/healthcare-cloud-computing-market.
- “2021 HIMSS Healthcare Cybersecurity Survey.” Healthcare Information and Management Systems Society. 2022. 2021_himss_cybersecurity_survey.pdf
- “7 Steps to Securing Health Care IoT Infrastructure.” n.d. Www.hfmmagazine.com. https://www.hfmmagazine.com/articles/3235-steps-to-securing-health-care-iot-infrastructure.

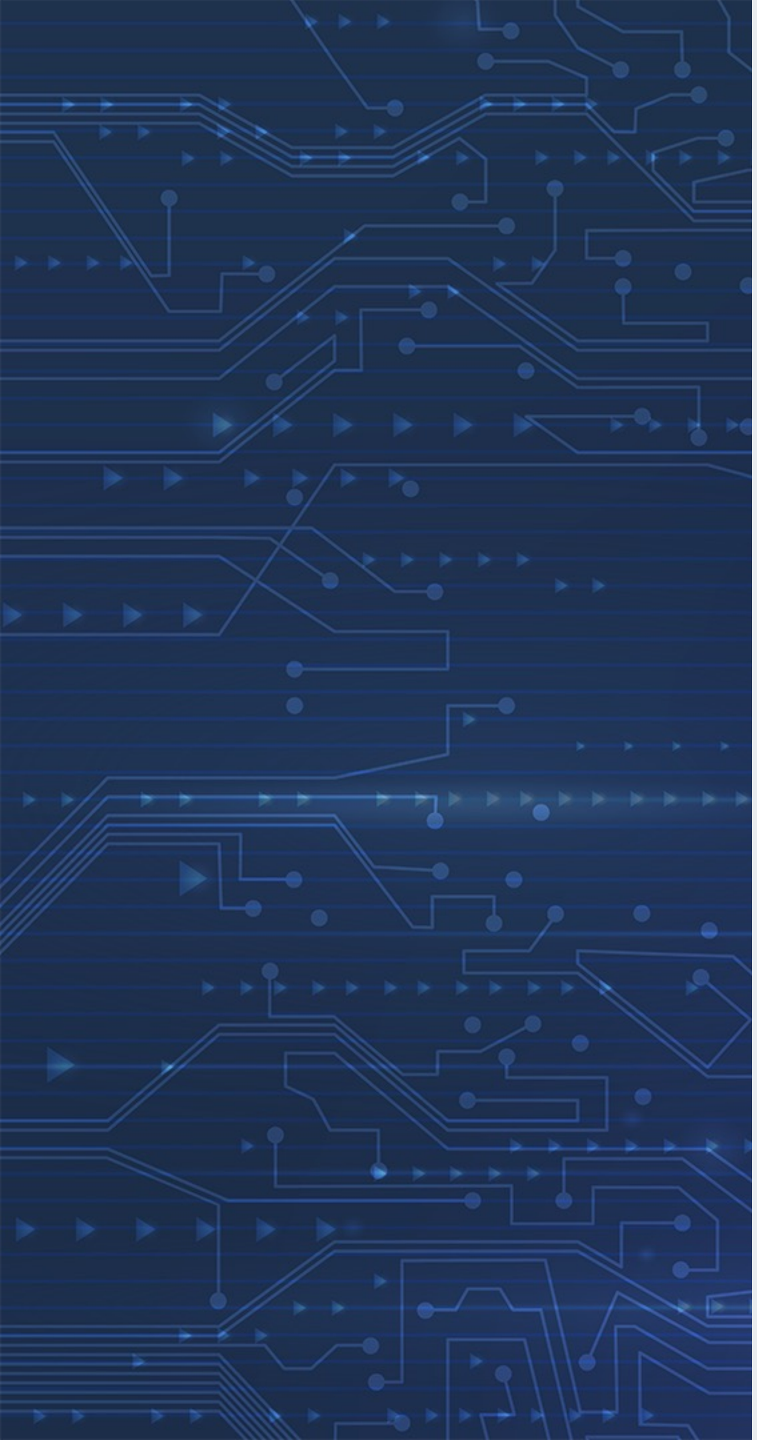
Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

WWW.HHS.GOV/HC3

HC3@HHS.GOV



Best Practices for Healthcare Cybersecurity Governance in the AI Age

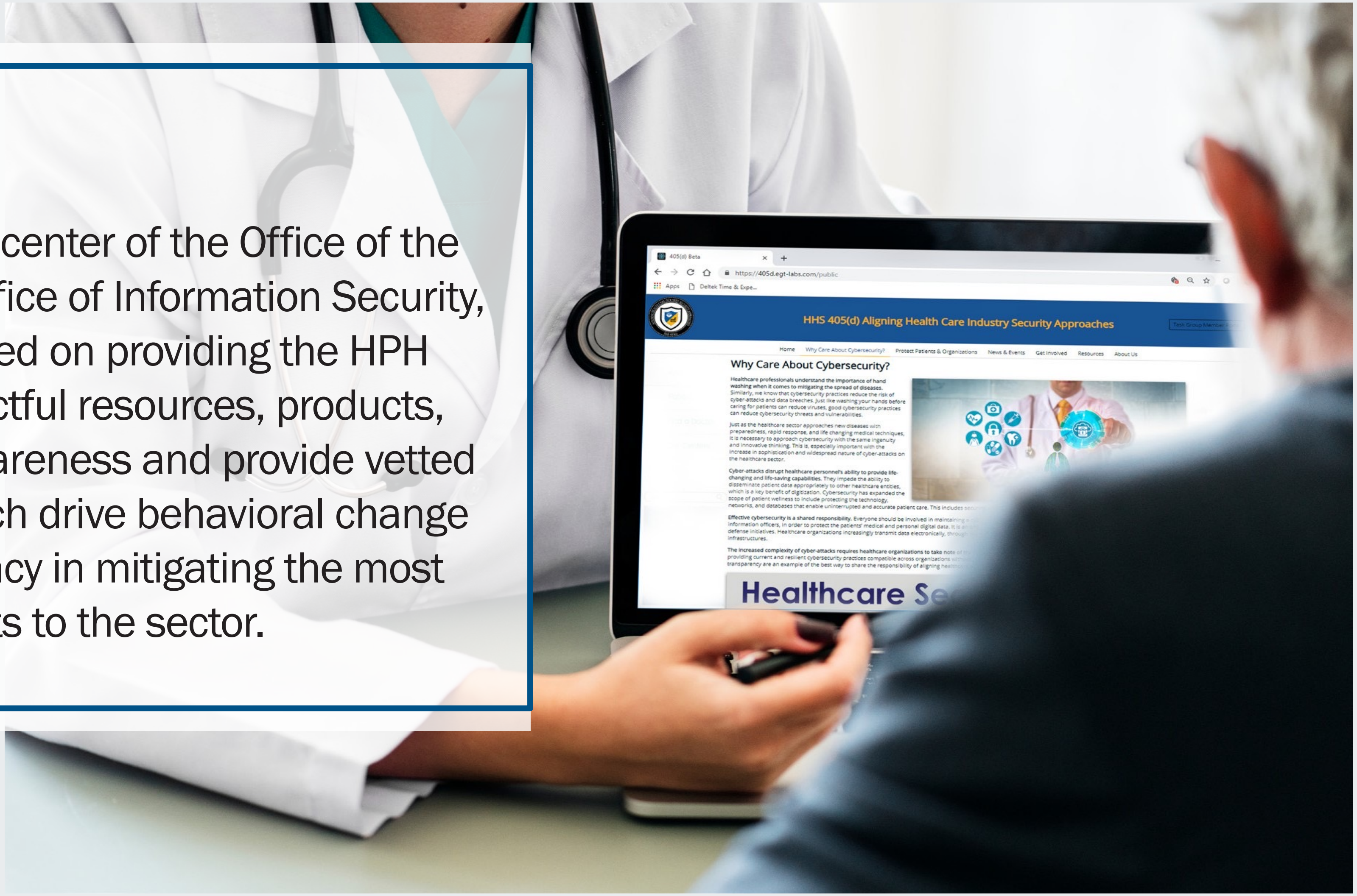
405(d) Program- (Speaker: Nick Rodriguez)

AI- (Speaker: Rahul Gaitonde)

Aligning Healthcare Industry Security Approaches

Mission

As the leading collaboration center of the Office of the Chief Information Officer/Office of Information Security, the 405(d) program is focused on providing the HPH sector with useful and impactful resources, products, and tools that help raise awareness and provide vetted cybersecurity practices, which drive behavioral change and move towards consistency in mitigating the most relevant cybersecurity threats to the sector.


HHS 405(d) Aligning Health Care Industry Security Approaches
Why Care About Cybersecurity?
Healthcare Se

405(d) Program Launches New Initiatives

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients 2023 Edition

The HICP publication was updated to include the most pertinent cybersecurity threats to the healthcare sector and the best practices needed to mitigate them.

Hospital Cyber Resiliency Initiative Landscape Analysis

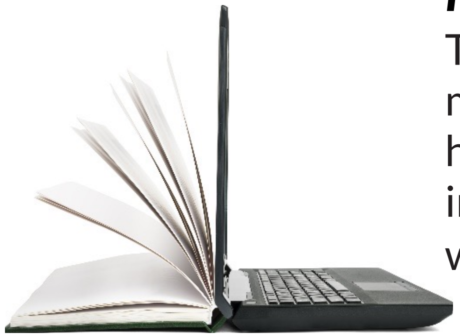
Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

CMS

HHS 405(d)
Aligning Health Care Industry Security Approaches

Hospital Cyber Resiliency Initiative Landscape Analysis

This analysis uses data from private and public partners to compare U.S. hospital systems' cybersecurity capabilities against the most prevalent methods cyber adversaries use to break in and cause disruptive attacks and then provides information on how to align these deficiencies to the HICP publication



Knowledge on Demand

This new cybersecurity education platform includes multiple delivery methodologies to reach the varied size health care facilities across the country. The platform includes five cybersecurity awareness trainings that align with the top five cybersecurity threats outlined in HICP

HICP 2023 Edition

The 405(d) Task Group has been working over the past 2 years to update HICP to ensure that the publication stays relevant and provides the sector with the most up-to-date best practices.

Updates were made across the Main Document and each of the ten practices in the technical volumes. Below is a list of the MAJOR updates.

Main Document updates Overview:

- The HICP Main Document has been updated to renew our call to action to maintain patient safety and includes new cybersecurity strategies such as **Zero Trust** and **Defense in Depth**.
- Email Phishing is now Social Engineering

Top Ten Practices Updates:

- Cybersecurity Practice #9 on Network Connected Medical Devices has been fully updated
- Cyber Practice #10 is now Cybersecurity Oversight and Governances

Additional NEW sub-practices have been included:

- Cyber insurance
- Cybersecurity Risk Assessment and Management
- Attack Simulations
- Medical Devices (Major Updates)

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

Healthcare & Public Health Sector Coordinating Council PUBLIC PRIVATE PARTNERSHIP

Volume 1: Cybersecurity Practices for Small Health Care Organizations

Healthcare & Public Health Sector Coordinating Council PUBLIC PRIVATE PARTNERSHIP

al Volume 2: ecurity Practices for Medium and Large Health Care Organizations

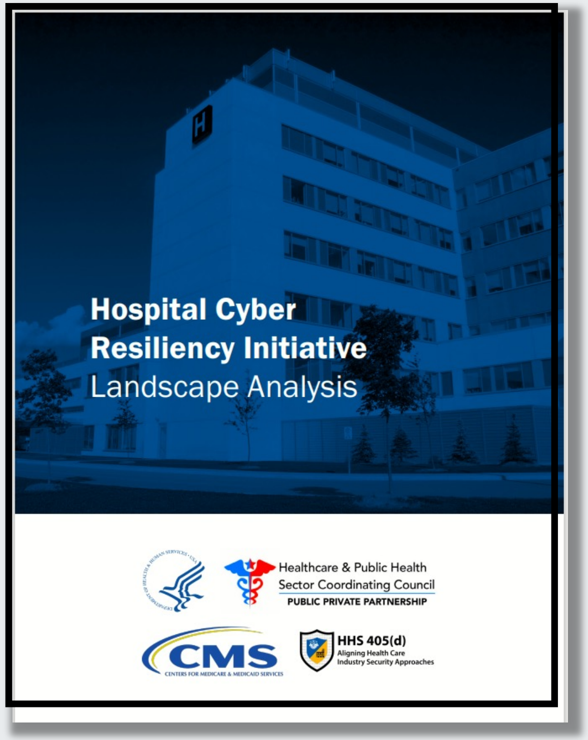
Healthcare & Public Health Sector Coordinating Council PUBLIC PRIVATE PARTNERSHIP

Hospital Cyber Resiliency Initiative Landscape Analysis

The HPH Sector has faced dramatic increases in cyber-attacks intended to cause disruption to the care continuum. In response to this growing threat, the HHS 405(d) Program conducted a Landscape Analysis, which reviewed active threats attacking hospitals and the cybersecurity capabilities of hospitals operating in the United States.

The analysis of the data sources shows that participating hospitals’ adoption of HICP practices fall into the following four categories:

- **No Action Required – Significant Progress Made**
  - Email protection systems
- **Urgent Improvement Needed**
  - Endpoint protection systems
  - Access management
  - Network management
  - Vulnerability management
  - Incident response
- **Additional Research Required**
  - Asset management
  - Medical device security
  - Cybersecurity policies
- **Further Attention Recommended (Not Urgent)**
  - Data protection and loss prevention



Hospital Cyber Resiliency Initiative Landscape Analysis

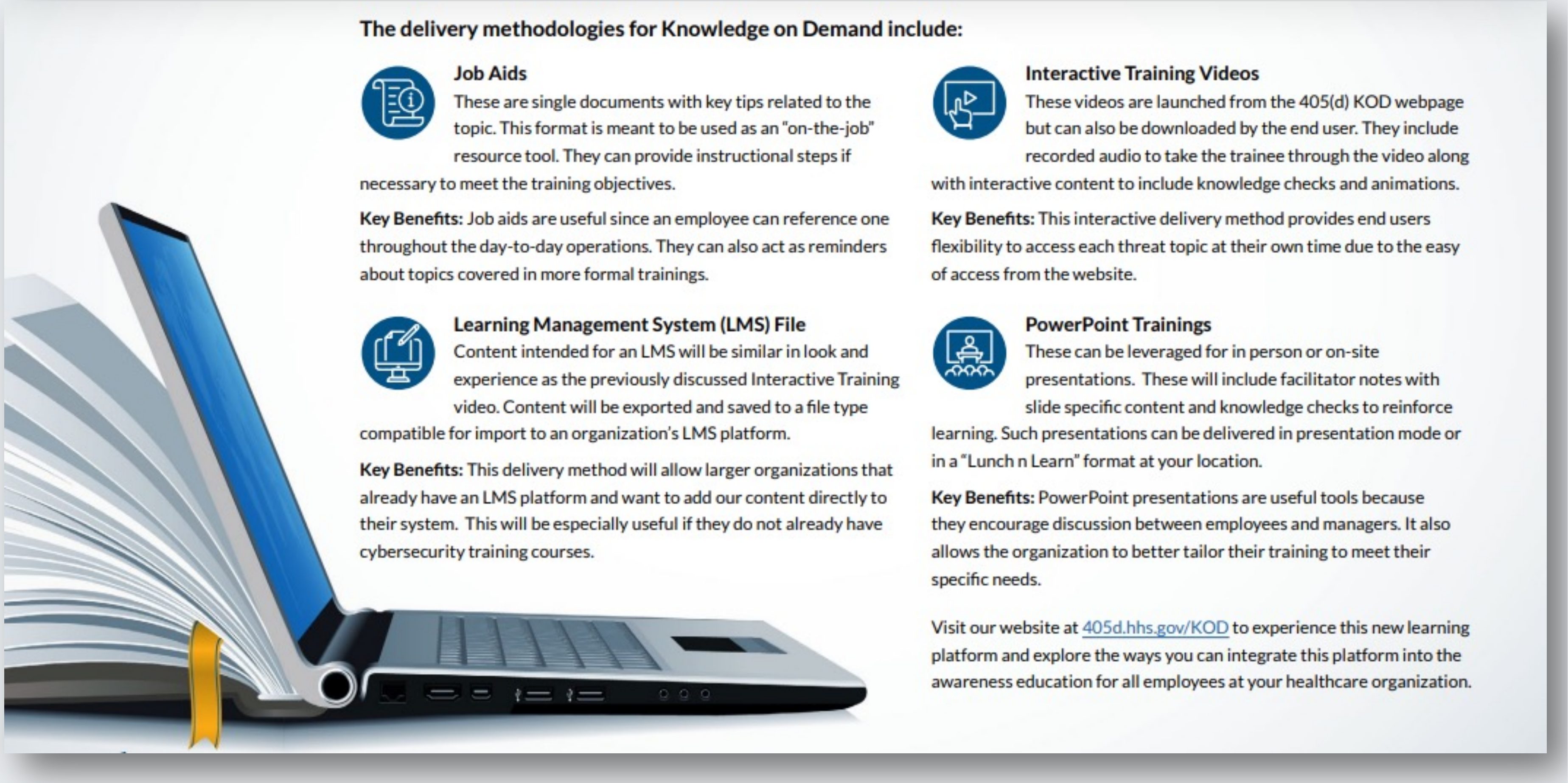
Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

HHS 405(d)
Aligning Health Care Industry Security Approaches

405(d) Knowledge on Demand

This new cybersecurity education platform includes multiple delivery methodologies to reach the varied size healthcare facilities across the country. The platform includes five cybersecurity awareness trainings that align with the top five cybersecurity threats outlined in the landmark 405(d) publication: *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)* and its accompanying two volumes.



The delivery methodologies for Knowledge on Demand include:

Job Aids

These are single documents with key tips related to the topic. This format is meant to be used as an "on-the-job" resource tool. They can provide instructional steps if necessary to meet the training objectives.

Key Benefits: Job aids are useful since an employee can reference one throughout the day-to-day operations. They can also act as reminders about topics covered in more formal trainings.

Learning Management System (LMS) File

Content intended for an LMS will be similar in look and experience as the previously discussed Interactive Training video. Content will be exported and saved to a file type compatible for import to an organization's LMS platform.

Key Benefits: This delivery method will allow larger organizations that already have an LMS platform and want to add our content directly to their system. This will be especially useful if they do not already have cybersecurity training courses.

Interactive Training Videos

These videos are launched from the 405(d) KOD webpage but can also be downloaded by the end user. They include recorded audio to take the trainee through the video along with interactive content to include knowledge checks and animations.

Key Benefits: This interactive delivery method provides end users flexibility to access each threat topic at their own time due to the easy of access from the website.

PowerPoint Trainings

These can be leveraged for in person or on-site presentations. These will include facilitator notes with slide specific content and knowledge checks to reinforce learning. Such presentations can be delivered in presentation mode or in a "Lunch n Learn" format at your location.

Key Benefits: PowerPoint presentations are useful tools because they encourage discussion between employees and managers. It also allows the organization to better tailor their training to meet their specific needs.

Visit our website at 405d.hhs.gov/KOD to experience this new learning platform and explore the ways you can integrate this platform into the awareness education for all employees at your healthcare organization.

Office of
Information Security
Securing One HHS

405(d) Outreach & Program Resources

Staying Cyber Safe in the Healthcare and Public Health Sector
Tips for individuals and organizations

HHS 405(d)

Why is healthcare targeted?

Where do these attacks come from?

Cyber Hygiene Tips:

HHS/405(d) Awareness Materials

The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! Since 2018 the program has released more than 60 awareness products which organizations across the HPH sector can leverage.

405(d) Outreach

The 405(d) Program produces Bi-monthly Newsletters, SBARs, and Spotlight Webinars to increase cybersecurity awareness and present new and emerging cybersecurity news and topics, as well highlight the HICP Publication!

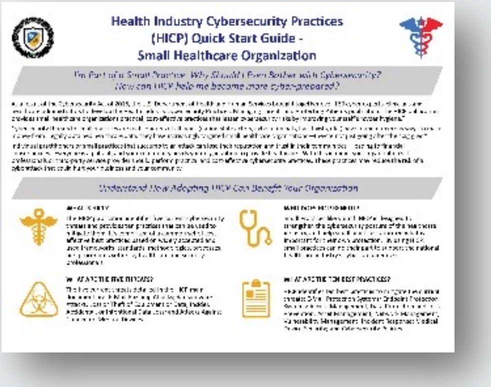
405(d) Program Presents:

A Case Study of "Cancer Care in the Wake of a Cyber Attack"

Aligning Health Care Industry Security Approaches

Knowledge on Demand

The 405(d) Program, is launching a new cybersecurity training platform on its website—405d.hhs.gov.This new cybersecurity education platform will include multiple delivery methodologies to reach the varied size health care facilities across the country. The platform will include five cybersecurity awareness trainings that align with the landmark 405(d) publication: HICP and its accompanying two volumes.



Health Industry Cybersecurity Practices (HICP) Quick Start Guide - Small Healthcare Organization

I'm Part of a Small Practice. Why Should I Even Bother with Cybersecurity? How can HICP help me become more cyber-prepared?

Understand How Adopting HICP Can Benefit Your Organization

Official Task Group Products

These resources are official products produced by the 405(d) Task Group. Examples include the HICP Publication, Quick Start Guides, New Cyber ERM Publication, and 5 threat flyers.

Office of
Information Security
Securing One HHS

Subscribe and Join!

Do you follow us on Social Media?
Check us out at @ask405d

Visit our website 405d.hhs.gov

Want to lend your voice to our discussions? Join our Task Group!

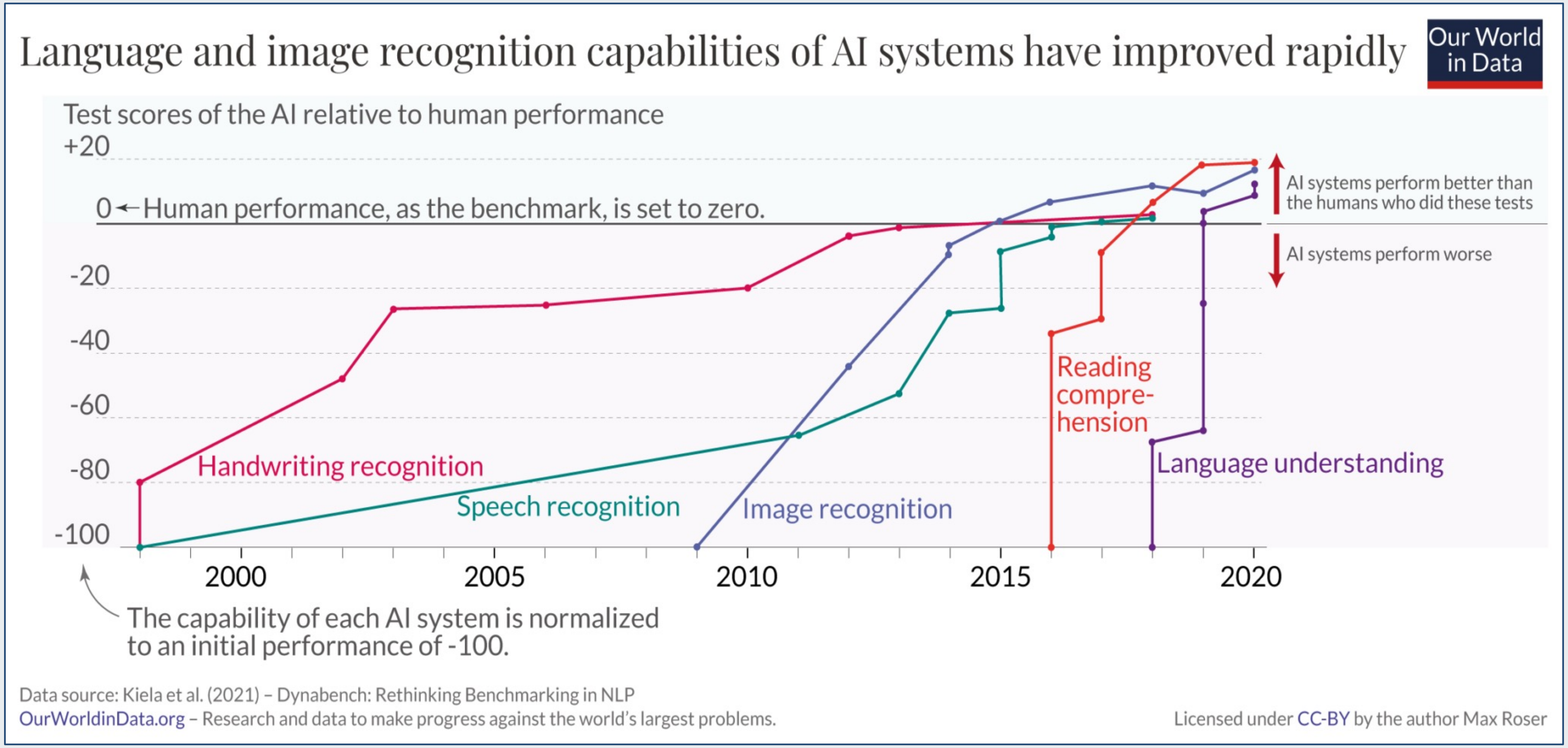
ALIGNING HEALTH CARE INDUSTRY SECURITY APPROACHES
HHS 405(d)

Artificial Intelligence

Context

- **The White House is leading the development of a national AI strategy,** of which HHS has significant equities.
  - The White House is working on an AI executive order and OMB memorandum.
- **The HHS has been involved in AI in numerous ways over the past several years,** with particular foci on research (NIH), algorithm approvals (FDA), standards development (ONC), preparedness (ASPR, CDC), and more.
- **New capabilities have emerged (e.g., generative AI) in recent months, posing both great opportunity and risk.**
- **In the coming months, the HHS will work with OpDiv leadership to develop its own strategy,** identifying sets of use cases, governance models, regulatory considerations, and more for the Department to continue to lead on AI.

The Evolution of AI



Language and image recognition capabilities of AI systems have improved rapidly

Data source: Kiela et al. (2021) – Dynabench: Rethinking Benchmarking in NLP
OurWorldinData.org – Research and data to make progress against the world's largest problems.

Why AI Matters

- 2023 represents a historically unique moment for leadership in AI:
  - America's leadership in global scientific and economic competitiveness hinges on upfront leadership on AI; perfection cannot be the enemy of progress on AI development and deployment.
  - Available computer power to train and deploy models has grown exponentially over the past three years.
  - Convergence of factors accelerating path to adoption, e.g., growth in cloud computing, infrastructure improvements, new technology, cryptocurrency deployment, and pandemic investments.
- AI carries potentially disruptive upsides in health and human services, e.g., scientific discovery, increased system and administrative efficiency, clinical decision support, and health and human services benefit design and delivery.
- Health AI has experienced explosive growth over the past five years:
  - Significant increase in venture capital and private health AI investments in the past five years, with 40%+ CAGR; projected to reach ~$45B by 2026.
  - Generative AI is projected to grow faster in healthcare than any other industry.
  - AI's computational power is doubling every six to ten months.

Risks and Considerations

- **Ethical and responsible AI:**
  - **Ethical considerations:** Data privacy, accountability, bias; hypotheses or ideas not ethical to pursue.
  - **Accuracy and reliability:** Training data used to develop the system is biased, incomplete or not factoring developments and complexities unique to health and human services.
  - **Equity:** AI outputs could reinforce disparities.
  - **Trustworthiness:** Underlying algorithms are complex and not well-understood, as well as difficult to validate.
  - **Authorship, attribution, and ownership:** AI as contributing authors.
- **AI and the economy:**
  - **Centralized power:** Algorithm and tool owners could 'monopolize' economic potential of AI.
  - **Intellectual property:** Training on copyrighted or proprietary data.
  - **Access:** Higher resourced institutions and individuals may have greater access to the full benefits of AI.
  - **Price discrimination** could be accelerated by AI.
- **Geopolitical and economic competitiveness**

AI Usage Considerations

The Department is working on overall AI guidance. In the interim, the following represent some good practices for the safe usage of new AI tools:

- Do not share sensitive information (e.g., Personally Identifiable Information (PII) or Protected Health Information (PHI)) through publicly available AI chatbots.
- Do not use solely for decision-making or policymaking.
- Follow existing department policies on IT computer usage.
- The user is responsible for validating and checking all output.

Contact: HHS.CAIO@hhs.gov

More info: https://www.hhs.gov/about/agencies/asa/ocio/ai/index.html