LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

405(d) Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) Fireside Chat

February 2019

Agenda

Time	Topic	Speaker
5 Minutes	Opening Remarks & Introductions	
10 Minutes	CSA Section 405(d)'s Mandate, Purpose, and Desired Goals	Julie Anne Chua
15 Minutes	HICP Overview	Julie Anne Chua
15 Minutes	Using HICP and Supporting Resources	Erik Decker
10 Minutes	HICP's Value and Benefits	Erik Decker
10 Minutes	HICP Pretesting with Industry	Erik Decker
5 Minutes	Looking Forward	Julie Anne Chua
5 Minutes	Upcoming HICP Engagements	Julie Anne Chua
15 Minutes	Questions	

Presenters

Julie Chua – HHS Security Risk Management Division Branch Chief

Julie Chua serves as the Branch Chief of the Risk Management Program within the HHS Office of Information Security (OIS) She is responsible for establishing a Department-wide enterprise risk management program and overseeing high visibility/high priority initiatives including identification and protection of HHS' most critical high value assets and the HHS FedRAMP and Cloud Security Program. Julie also has a lead role in Healthcare and Public Health Sector public-private partnerships on many HHS cybersecurity initiatives to help push forward security and resiliency across the sector. Prior to joining OIS, Julie was the Cybersecurity Team Lead within the HHS Office of the National Coordinator for Health IT (ONC) leading Critical Infrastructure cybersecurity efforts.

Presenters

Erik Decker - Chief Security and Privacy Officer for the University of Chicago Medicine

Erik Decker is the Chief Information Security and Privacy Officer for the University of Chicago Medicine, and is responsible for its Cyber Security, Identity and Access Management and Privacy Programs. The majority of his career has been focused on Academic Medical Centers; establishing two information security programs and an identity and access management program. Erik is the industry lead for the CSA 2015 405d Task Group, responsible for the publication of the *Health Industry Cybersecurity Practices: Managing Threats and Protection Patients* reference guide (HICP). He is also a member of the Executive Council of the Health Sector Coordinating Council, and the previous Chair of the Association for Executives in Healthcare Information Security (AEHIS) Board.

CSA Section 405(d)'s Mandate, Purpose, and Desired Goals

Cybersecurity Act of 2015 (CSA): Legislative Basis

CSA Section 405

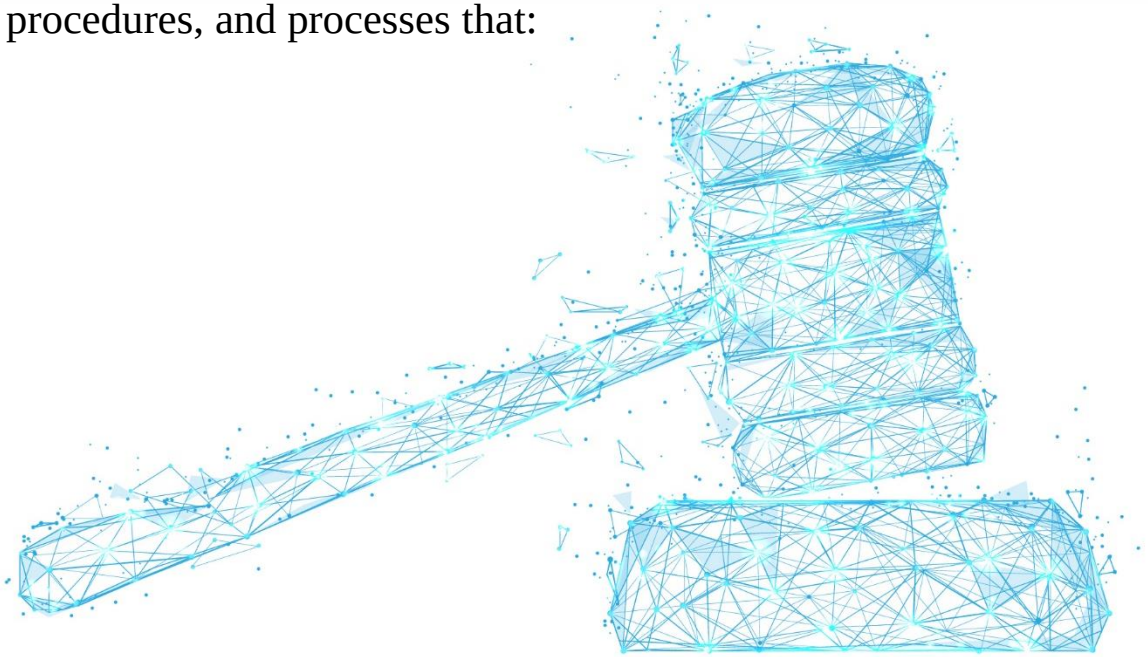
Improving Cybersecurity in the Health Care Industry

- Section 405(b): Health care industry preparedness report
- Section 405(c): Health Care Industry Cybersecurity Task Force
- **Section 405(d): Aligning Health Care Industry Security Approaches**

CSA Section 405(d): Legislative Language (1/2)

Authority: Cybersecurity Act of 2015 (CSA), Section 405(d), *Aligning Health Care Industry Security Approaches*

The Secretary shall establish, through a collaborative process with the Secretary of Homeland Security, health care industry stakeholders, the Director of the National Institute of Standards and Technology, and any Federal entity or non-Federal entity the Secretary determines appropriate, a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that:



CSA Section 405(d): Legislative Language (2/2)

A. Serve as a resource for *cost-effectively reducing cybersecurity risks* for a range of health care organizations;
B. Support *voluntary adoption and implementation* efforts to improve safeguards to address cybersecurity threats;
C. Are consistent with—
   i. The standards, guidelines, best practices, methodologies, procedures, and processes developed under section 2(c)(15) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)(15));
   ii. The security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d-2 note); and
   iii. The provisions of the Health Information Technology for Economic and Clinical Health Act (title XIII of division A, and title IV of division B, of Public Law 111-5), and the amendments made by such Act; and
D. Are updated on a regular basis and applicable to *a range of health care organizations*.

Industry-Led Activity to Improve Cybersecurity in the Healthcare and Public Health (HPH) Sector

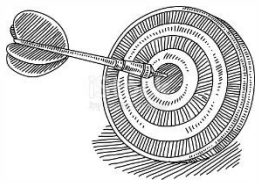
WHAT IS THE 405(d) EFFORT?

An industry-led process to develop consensus-based guidelines, practices, and methodologies to strengthen the HPH-sector's cybersecurity posture against cyber threats.

WHO IS PARTICIPATING?

The 405(d) Task Group is convened by HHS and comprised of over 150 information security officers, medical professionals, privacy experts, and industry leaders.

HOW WILL 405(d) ADDRESS HPH CYBERSECURITY NEEDS?



With a targeted set of applicable & voluntary practices that seeks to cost-effectively reduce the cybersecurity risks of healthcare organizations.

WHY IS HHS CONVENING THIS EFFORT?

To strengthen the cybersecurity posture of the HPH Sector, Congress mandated the effort in the Cybersecurity Act of 2015 (CSA), Section 405(d).

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

HICP Publication Overview

Document Objective and Development

Objective

The CSA 405(d) document aims to raise awareness, provide vetted practices, and foster consistency in mitigating the most pertinent and current cybersecurity threats to the sector. It seeks to aid the HPH sector organizations to develop meaningful cybersecurity objectives and outcomes.

Development

Leverage Existing Information

Existing information and guidance (e.g., NIST Cybersecurity Framework) was leveraged across the public and private domains to provide a tailored approach for the healthcare industry. It does not create new frameworks, re-write specifications, or "reinvent the wheel."

HPH Sector Public-Private Collaboration

To ensure a successful outcome and a collaborative process, HHS reached out to a diverse set of healthcare and cybersecurity experts from the public and private sectors. Participation is open and voluntary.

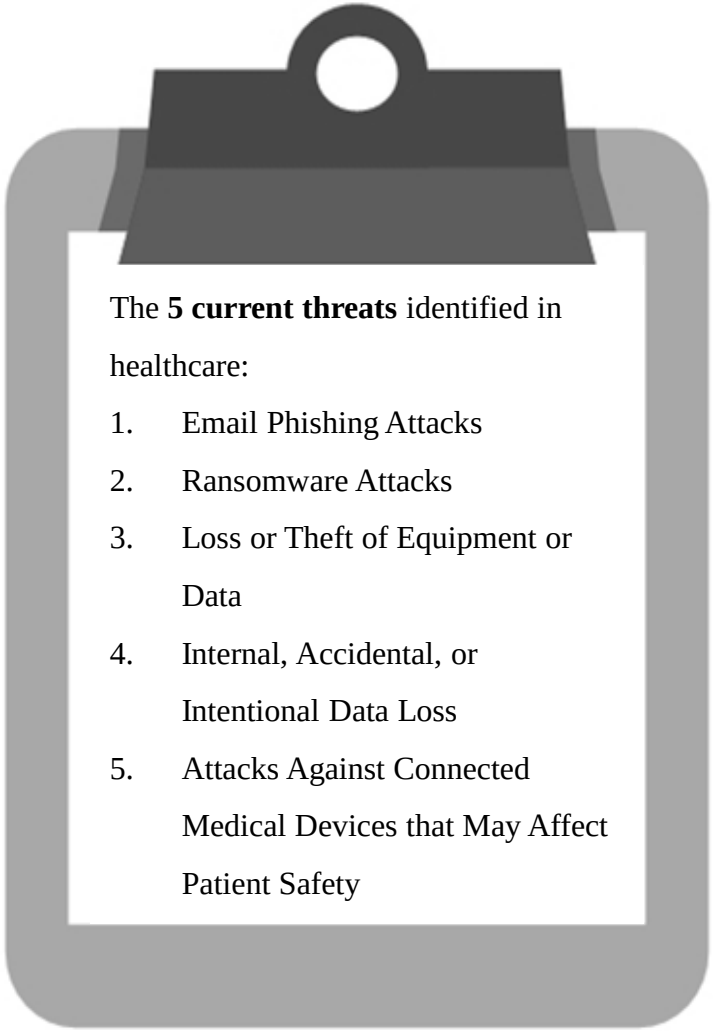
National Pretesting

Document Development Detail

Document - Content Overview (1/2)

After significant analysis of the current cybersecurity issues facing the HPH Sector, the Task Group agreed on the development of three documents—a main document and two technical volumes, and a robust appendix of resources and templates:

- The main document examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.
- *Technical Volume 1* discusses these ten cybersecurity practices for **small** healthcare organizations.
- *Technical Volume 2* discusses these ten cybersecurity practices for **medium and large** healthcare organizations.
- *Resources and Templates* provides mappings to the NIST Cybersecurity Framework, a HICP assessment process, templates and acknowledgements for its development.



Document - Content Overview (2/2)

The document identifies **ten (10) practices**, which are tailored to small, medium, and large organizations and discussed in further detail in the technical volumes:

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

Using HICP and Supporting Resources

Introduction and Executive Summary

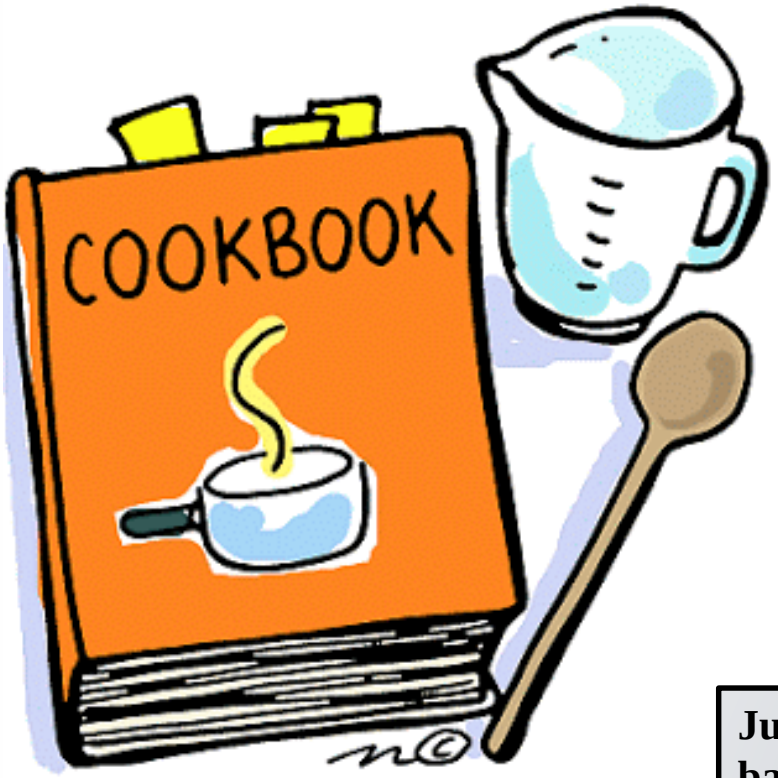
HICP is…

- A call to action to manage real cyber threats
- Written for multiple audiences (clinicians, executives, and technical)
- Designed to account for organizational size and complexity (small, medium and large)
- A reference to "get you started" while linking to other existing knowledge
- Aligned to the NIST Cybersecurity Framework
- Voluntary

HICP is **not**…

- A new regulation
- An expectation of minimum baseline practices to be implemented in all organizations
- The definition of "reasonable security measures" in the legal system
- An exhaustive evaluation of all methods and manners to manage the threats identified
  - You might have other practices in place that are more effective than what was outlined!
- Your guide to HIPAA, GDPR, State Law, PCI, or any other compliance framework

HICP is a Cookbook!



So you want a recipe for managing phishing?

1. 5 oz of Basic E-Mail Protection Controls (1.M.A)
2. A dash of Multi-Factor Authentication (1.M.B)
3. 2 cups of Workforce Education (1.M.D)
4. 1 cup of Incident Response plays (8.M.B)
5. 1 tsp of Digital Signatures for authenticity (1.L.B)
6. Advanced and Next General Tooling to taste (1.L.A)

Preheat your email system with some basic email protection controls necessary to build the foundation of your dish. Mix in MFA for remote access, in order to protect against potential credential theft.

Let sit for several hours, while providing education to your workforce on the new system, and how to report phishing attacks. While doing so, ensure to provide education on how digital signatures demonstrating authenticity of the sender. When finished baking, sprinkle with additional tooling to provide next level protection.

Just like with any cookbook the recipes provide the basic ingredients to making a meal. It does not:

- **Instruct you how to cook**
- **Instruct you on what recipes to use**
- **Limit your ability for substitutions**

The skill of the cook is what makes the dish!

How to Evaluate Your Organization's Size

HICP is designed to assist organizations of various sizes implement resources and practices that are tailored and cost effective to their needs.

- How "large and complex an organization you might be relates to several factors:
  - Health Information Exchanges
  - IT Capability
  - Cybersecurity Investment
  - Size (provider)
  - Size (acute/post-acute)
  - Size (hospital)
  - Complexity
- Determining where you fit is your decision

[Main Document](), p. 11

Medium

Best Fit		Small	Medium	Large
Common Attributes	Health information exchange partners	One or two partners	Several exchange partners	Significant number of partners or partners with less rigorous standards or requirements Global data exchange
	IT capability	No dedicated IT professionals on staff, IT may be outsourced on a break/fix or project-by project-basis	Dedicated IT resources on staff No or limited dedicated security resources on staff	Dedicated IT resources with dedicated budget CISO or dedicated security leader with dedicated security staff
	Cybersecurity investment	Nonexistent or limited funding	Funding allocated for specific initiatives Potentially limited future funding allocations Cybersecurity and IT budgets are blended	Dedicated budget with strategic roadmap specific to cybersecurity
Provider Attributes	Size (provider)	1–10 physicians	11–50 physicians	Over 50 physicians
	Size (acute / post-acute)	1–25 providers	26–500 providers	Over 500 providers
	Size (hospital)[15]	1–50 beds	51–299 beds	Over 300 beds
	Complexity	Single practice or care site	Multiple sites in extended geographic area	Integrated delivery networks Participate in accountable care organization or clinically integrated network
Other Org Types			Practice Management Organization Managed Service Organization Smaller device manufacturers Smaller pharmaceutical companies Smaller payor organizations	Health Plan Large Device Manufacturer Large pharmaceutical organization

Table 1. Selecting the "Best Fit" For Your Organization

How to Use Practices and Sub-Practices

- There are a total of **10** Cybersecurity Practices, and **89** Sub-Practices.
- Each Cybersecurity Practice has a corresponding set of Sub-Practices, risks that are mitigated by the Practice, and suggested metrics for measuring the effectiveness of the Practice
- Medium Sized orgs can review the Medium Sub-Practices
- Large Sized orgs can review the Medium **and** Large Sub-Practices
- Each Practice is designed to mitigate one or many threats

Cybersecurity Practice 2: Endpoint Protection Systems	
Data that may be affected	Passwords, PHI
Medium Sub-Practices	2.M.A Basic Endpoint Protection Controls
Large Sub-Practices	2.L.A Automate the Provisioning of Endpoints 2.L.B Mobile Device Management 2.L.C Host Based Intrusion Detection/Prevention Systems 2.L.D Endpoint Detection Response 2.L.E Application Whitelisting 2.L.F Micro-segmentation/virtualization strategies
Key Mitigated Risks	• Ransomware Attacks • Theft or Loss of Equipment or Data

Sample Metrics

- Percentage of endpoints encrypted based on a full fleet of known assets, measured weekly.
- Percentage of endpoints that meet all patch requirements each month.
- Percentage of endpoints with active threats each week.
- Percentage of endpoints that run non hardened images each month.
- Percentage of local user accounts with administrative access each week.

Suggested Assessment Process

Resources and Templates, p. 39

Prioritize Your Threats (with Example)

- Implementing all Practices within HICP could be daunting, even for a Large Sized Organization
- Recommendation: Review the threats and implement the most impactful practices first
  - A toolkit will be released shortly to assist with this process

Factor		
Select your organizations size		Medium
Prioritize the threats (5 being highest priority, 1 being lowest priority)		
A	Email Phishing Attack	1
B	Ransomware Attack	4
C	Loss or Theft of Equipment or Data	5
D	Insider, Accidental or Intentional Data Loss	3
E	Attacks Against Connected Medical Devices that may affect Patient Safety	2

CP #	Cybersecurity Practices	Priority Rank Based on Threat Model Inputs
8	Incident Response	28
3	Access Management	23
2	Endpoint Protection Systems	23
5	Asset Management	20
6	Network Management	16
7	Vulnerability Management	16
10	Cybersecurity Policies	15
1	Email Protection Systems	13
9	Medical Device Security	11
4	Data Protection and Loss Prevention	11

Self-Assessment to Practices (with Example)

Continuing with the example previously, we have selected the top 3 practices and sub-practices to help mitigate Loss or Theft of Equipment or Data

FULL LISTING OF CYBERSECURITY SUB-PRACTICES BASED ON ORGANIZATION SIZE SELECTED			Self Assessment			
SP#	**Cybersecurity Sub-Practice Title**	**Short Description**	**Current State**	**Gaps**	**Action Plan**	**Priority**
2.M.A	Basic Endpoint Protection Controls	Basic endpoint security controls to enable	*Encryption at 80%, AV in place, baseline image, all users with admin rights*	*Encryption gaps and admin rights*	*Finish encryption, remove admin rights*	*High*
3.M.A	Identity	Establish a unique identifier for all users, leveraging systems of record	*All users provided accounts, not tied to ERP*	*No identity, can allow for orphaned accounts and failure to term*	*Establish identity program*	*Me*
3.M.B	Provisioning, Transfers, and De-provisioning Procedures	Provision user accounts based on identity; ensure de-provisioning upon termination	*User accounts created directly into Active Directory manually, when requested*	*Access rights might cumulate and administrators might fail to terminate access*	*Establish accounts based upon identity, automate provisioning and de-provisioning*	*Med*
3.M.C	Authentication	Implement and monitor secure authentication for users and privileged accounts	*Authentication bound to central authentication source*	*No gaps*	*No gaps*	*N/A*
3.M.D	Multi-Factor Authentication for Remote Access	Implement multi-factor authentication for remote access to resources	*VPN access available, no MFA*	*No MFA enabled, which can allow for a theft of credentials to access sensitive data*	*Implement MFA*	*Med*
8.M.A	Security Operations Center	Establish a SOC to prevent, discover and respond to cyber attacks	*Dedicated team to manage and respond to cyber incidents*	*No gaps*	*No Gaps*	*N/A*
8.M.B	Incident Response	Establish formal incident response playbooks for responding to cyber attacks	*Playbooks exist, but no playbook for lost/stolen device*	*In the case of a stolen device teams might not execute investigation properly*	*Establish playbook for stolen devices, get approval from leadership*	*High*
8.M.C	Information Sharing and ISACs/ISAOs	Join security communities to share best practices and threat information	*Not a current member of an ISAC/ISAO*	*By not participating in ISAC/ISAOs cyber teams might be missing out on leading practices*	*Join ISAC/ISAO*	*High*

Cybersecurity Practices Assessment Toolkit

Example Assessment (Appendix E)

Step	Analysis	Outcome
Step 1: Threat Assessment	Reviewed all threats. Threat most likely to occur is Phishing.	Determined that phishing attacks could cause the most damage to the organization. Start here.
Step 2: Review Practices	Reviewed all 10 Practices.	Identified three practices that would help mitigate this threat: Email Phishing Protection, Security Operations Center / Incident Response (SOC/IR), Policies and Procedures
Step 3: Determine Gaps	Reviewed the sub-practices identified within the three practices.	Email phishing protection controls are sufficient. No education or phishing simulation conducted.
Step 4: Identify Improvement Opportunities and Implement	Phishing education comes with no direct costs. Phishing simulations would be too expensive for the small practice.	Deferred the implementation of Phishing simulation. Established a workforce phishing education program and implemented.
Step 5: Repeat	Reviewed additional 4 threats, determined next most critical is ransomware.	Start the process anew.

Table 3. A Small Provider Practice Applies the Five-Step Process to a Phishing Attack Scenario

Resources and Templates, p. 41

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

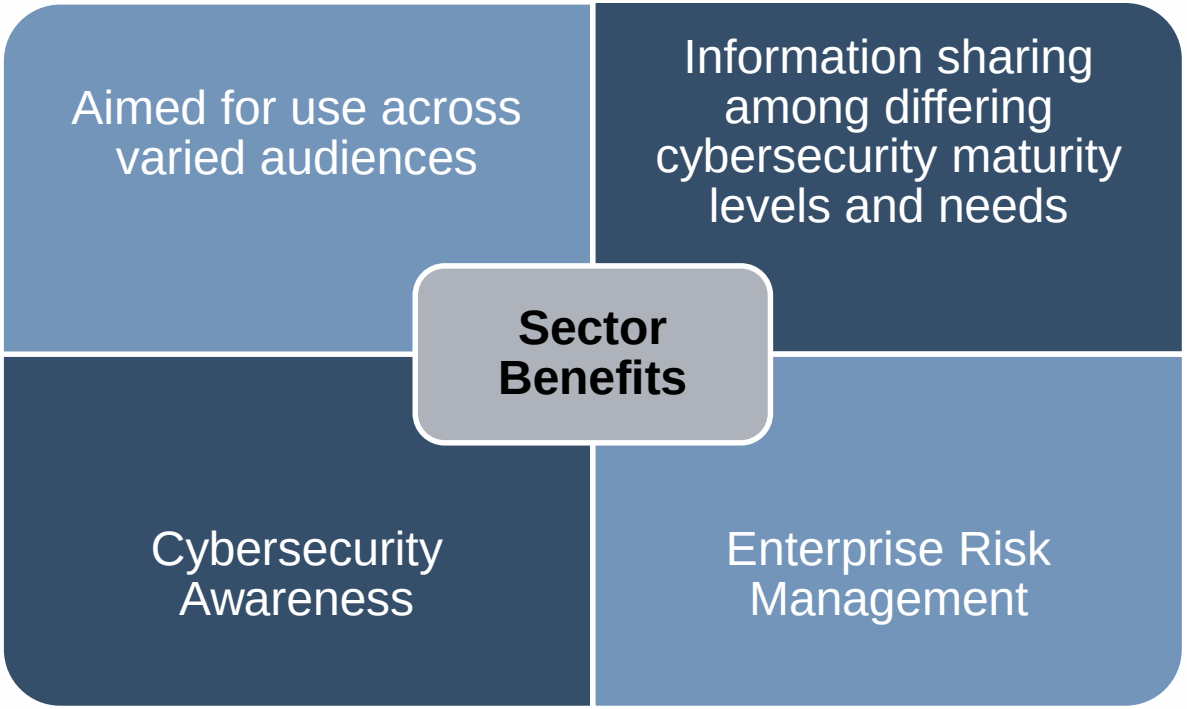
Value and Benefits

Healthcare and Public Health (HPH) Sector Benefits

This joint HHS- and industry- led initiative aims to increase awareness and foster consistency with cybersecurity practices for a wide range of stakeholders.

Executives
Practitioners
InfoSec
Users

It is critical for uninterrupted care delivery and patient safety

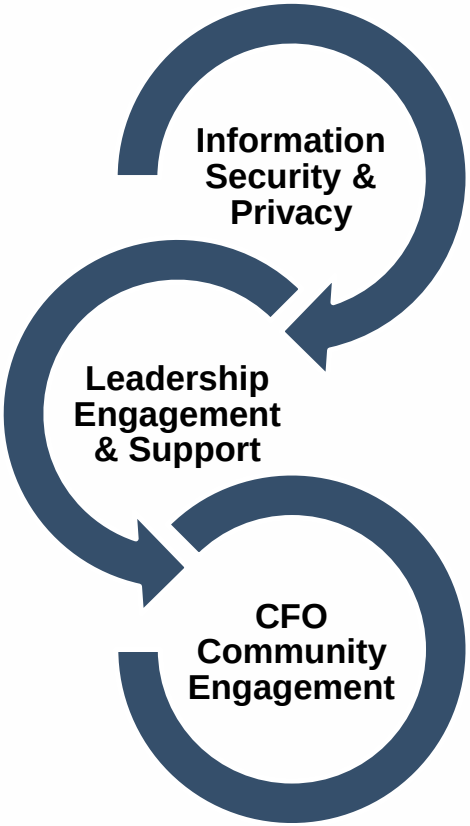


Small, medium, and large healthcare organizations can vary in their level of cybersecurity maturity and needs

Cybersecurity should be treated as an enterprise issue, not just an IT issue

Cybersecurity: An Enterprise Issue

HHS continues to institutionalize cybersecurity as a key priority and is actively advocating the culture shift to treat cybersecurity as an enterprise issue.



HHS has Healthcare and Public Health (HPH) Sector-Specific Agency responsibilities for all hazards including cybersecurity and public-private partnerships.

Continued engagement with the Enterprise Risk Management (ERM) community and senior/executive leadership on cybersecurity activities, strategies, and risk management.

As ERM matures within the healthcare industry, continued support is needed to operationalize cybersecurity and information security risks as part of our strategic, mission, and business risk management decisions across HHS and the HPH sector.

LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

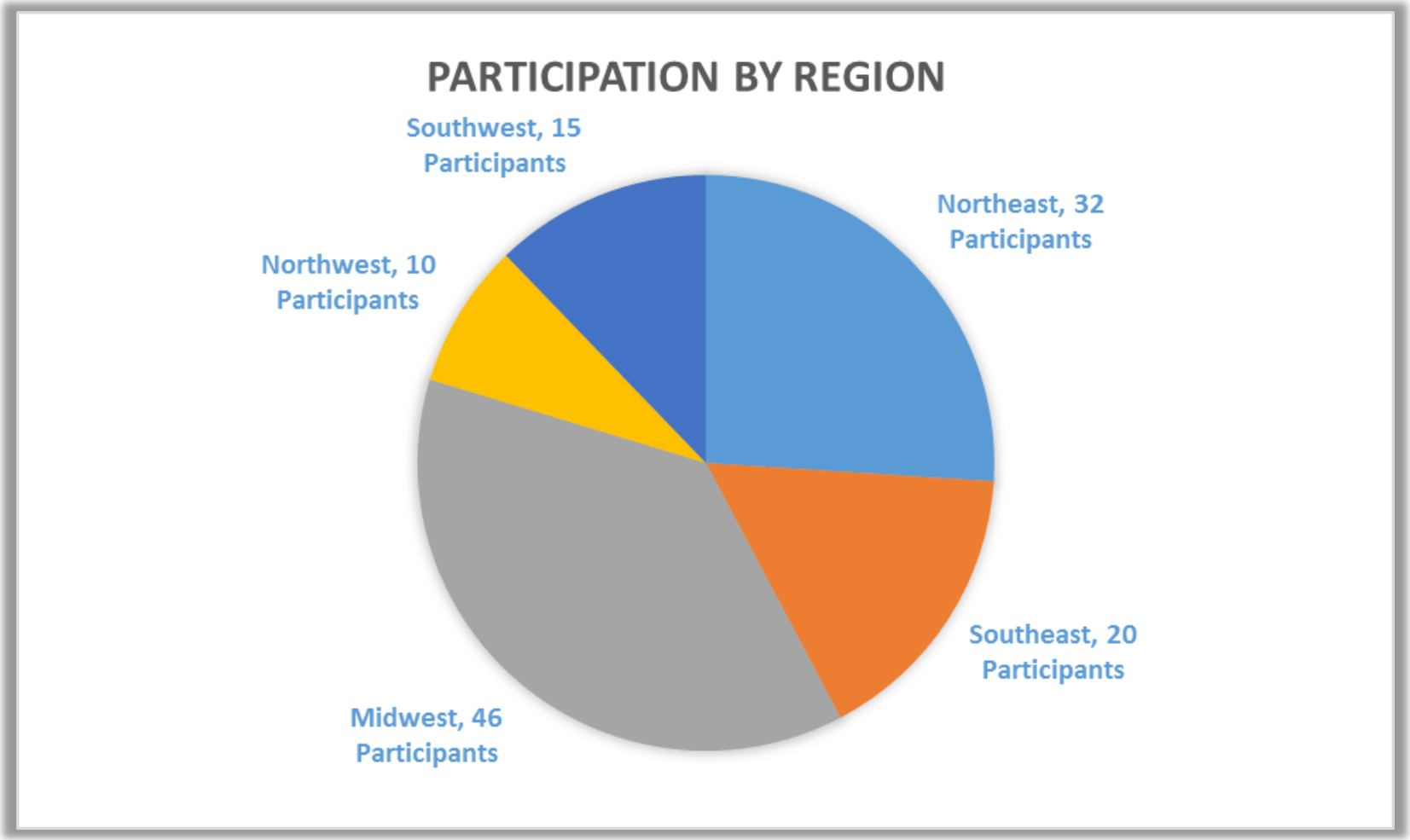
Pretesting Findings

Pretesting Background

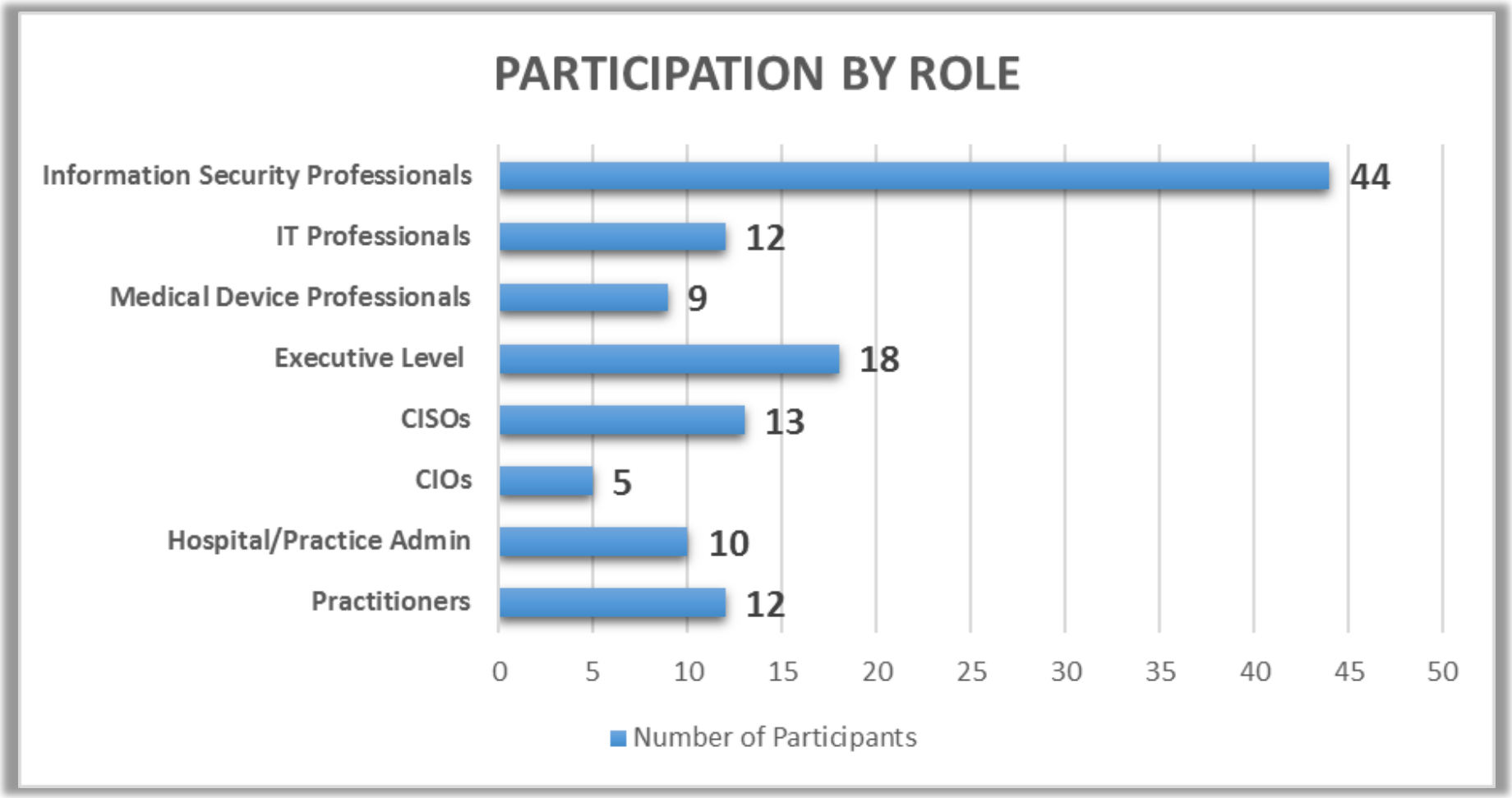
Pretesting of the 405(d) document consisted of facilitated focus group discussions assessing the practicality, usability, and what impact this document can have. Stakeholder groups included Medical Professionals, HPH CIOs/CISOs, and other HPH staff.

Pretesting sessions were both in-person and virtual, and feedback was gathered with focus groups of 9-15 participants via roundtable discussion. Comments were well received and incorporated into the initial publication, if applicable. Outstanding comments have been captured for future reference.

Pretesting: By Region

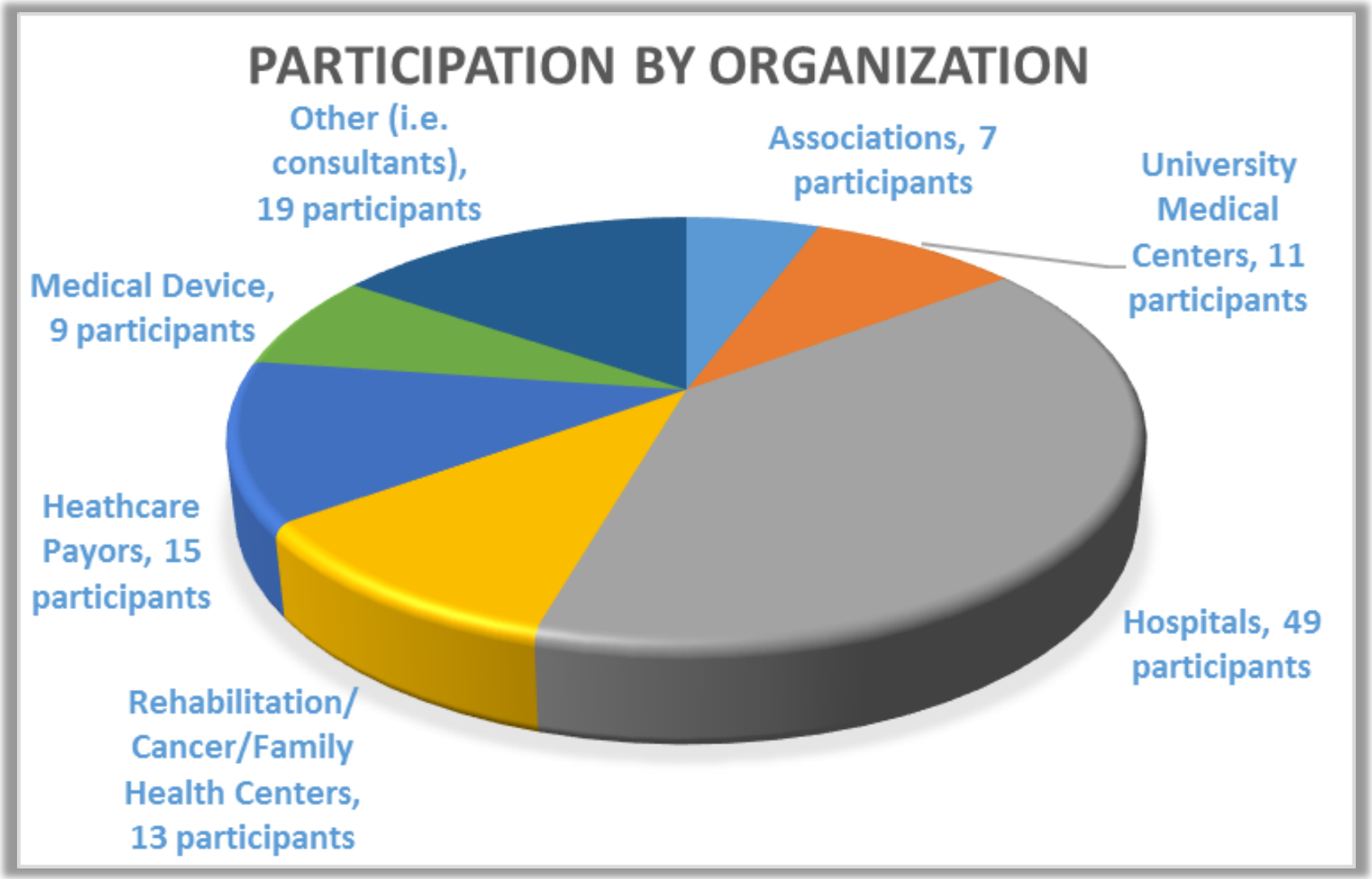


Pretesting: By Role



123 Total Participants

Pretesting: By Organization



Looking Forward

Looking Forward

CSA 405(d) aims to be the leading collaboration center of OCIO/OIS, in partnership with HHS Divisions, and the healthcare industry focused on the development of resources that help align health care cybersecurity practices

- **Immediate Next Steps**
  - Over the course of the next year the 405(d) Team plans to continue to develop awareness of the HICP publication and engage with stakeholders by:
    - Building additional supporting materials/resources to spotlight the HICP publication and related content
    - Develop means to collect feedback and implementation of HICP practices and methods
    - Hosting additional outreach engagements

Upcoming HICP Engagements

HICP's Five Threats Weekly Series

- **Background**
  - The HICP Five Threats Weekly Series hosted by the 405(d) Initiative is a series of presentations focused on the Five Threats identified in the publication. The HICP document and its supporting materials provides the healthcare community with a new resource to help strengthen their posture against cyber threats. These *hour and half long presentations* will allow the community to dive deeper into the Five threats individually and their corresponding mitigation practices.
- **Dates of Engagement**
  - Week 1/Threat 1 – E-mail Phishing Attack: **March 19 & 21, 2019**
  - Week 2/Threat 2 – Ransomware Attack: **March 26 & 28, 2019**
  - Week 3/Threat 3 – Loss or Theft of Equipment or Data: **April 2 & 4, 2019**
  - Week 4/Threat 4 – Insider, Accidental or Intentional Data Loss: **April 9 & 11, 2019**
  - Week 5/Threat 5 – Attacks Against Connected Medical Devices: **April 16 & 18, 2019**
- **Want to Receive Five Threats related Communication?**
  - Visit the 405(d) Website and sign up to receive email notifications from us regarding the Five Threat Weekly Series and other related information

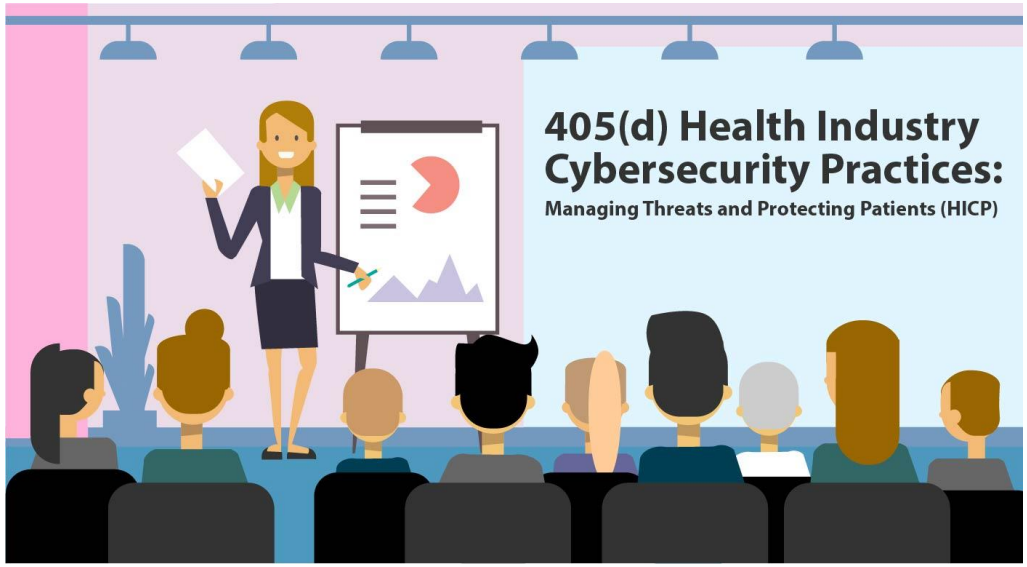
Come Hear Us Speak

Throughout 2019 the 405(d) Team will be traveling around the country and speaking at different industry focused conferences to promote our collaborative initiative and deliver in-person awareness of the HICP publication.

- HIMSS19 Global Conference & Exhibition - February 11-15, 2019 Orlando, FL
  - Speaking on February 12th, 2019
  - Session #82, 4:15-5:15pm
  - Come visit us at The

    Federal Health IT Pavilion

Check our Website for any new Announcements and future Speaking Engagements!



Questions

Thank you for Joining Us

Visit us at: www.phe.gov/405d

Contact Us at: CISA405d@hhs.gov