THE LEADING HEALTH INFORMATION AND TECHNOLOGY CONFERENCE

HIMSS19 | CHAMPIONS OF HEALTH UNITE

Global Conference & Exhibition FEB 11–15, 2019 | ORLANDO

Overview of 405d Publication - Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)

Health and Human Services Cybersecurity Program

Disclosure

Erik Decker

Julie Chua

Have no real conflicts

Learning Objectives

- Describe the public-private partnership model developed between the Healthcare Sector Coordinating Council and the Government Coordinating Council
- List the 5 cybersecurity threats the industry feels are most critical to manage
- Identify the 10 cybersecurity practices to mitigate these threats, and their sub-practices
- Discuss how to prioritize the threats for your organization, and subsequently the implementation of practices to mitigate these threats

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

Cybersecurity Act of 2015 (CSA): Legislative Basis

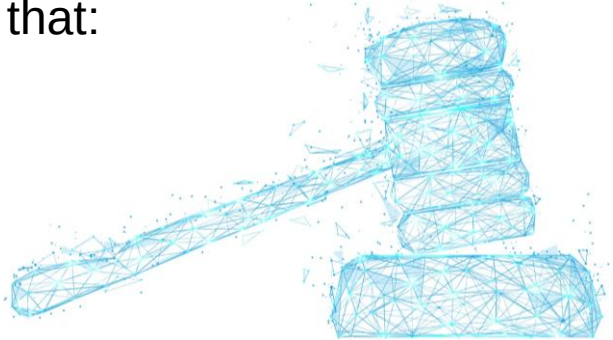
CSA Section 405

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

Cybersecurity Act of 2015 (CSA): Legislative Basis

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:



Cybersecurity Act of 2015 (CSA): Legislative Basis Continued

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 updated on a regular basis and applicable to *a range of health care organizations;*

D. 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;

ii. The security and privacy regulations promulgated under section 264(c) of the Health Insurance Portability and Accountability Act of 1996;

iii. The provisions of the Health Information Technology for Economic and Clinical Health Act

HIMSS19 | CHAMPIONS OF HEALTH UNITE

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

#HIMSS19

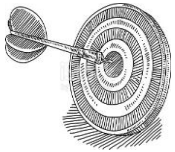
WHAT IS THE 405(d) EFFORT?

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).

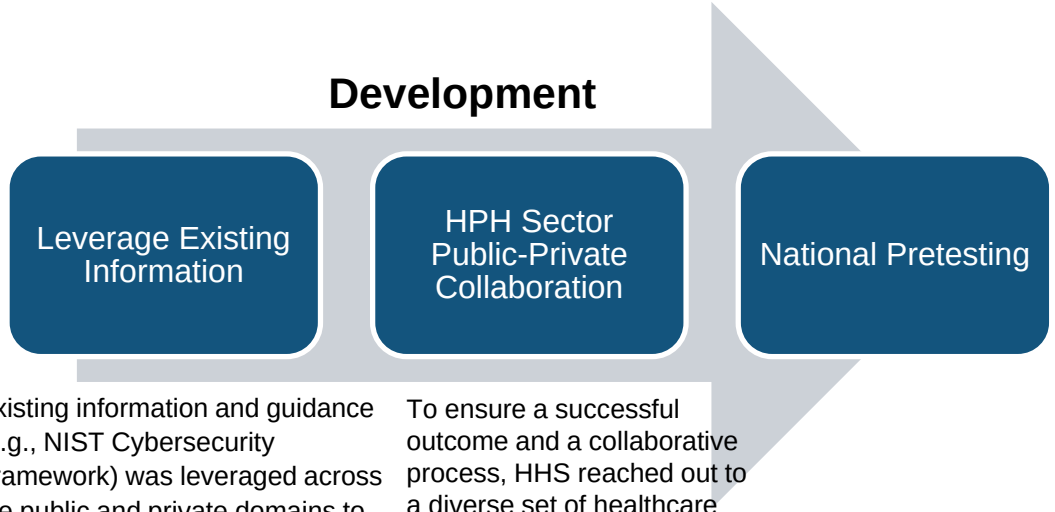
HICP Overview

Document Overview & Development

Overview

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



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.”

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.

Document Development Detail

Identified ~**110 members**. **Convened 6 times** from May 2017 to March 2018

Administrative Support and **Writing Counsel**

4 Subgroups collaboratively developed **96 page annotated outline**

3 Focus Group Assessments
19 total participants including healthcare and CIOs/CISOs

35 One-on-One Interviews with Task Group Members

Deliberation and consensus **resulting in Writing Committee's new 34 page format**

Group interviews with medical professionals and HPH CIOs/CISOs.

Quantitative and qualitative **knowledge-base for HPH Sector**.

Qualitative Research to **Establish Level of Awareness** and Prioritization

Document Content Overview

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:

- 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.

The **5 current threats** identified in healthcare:

1. Email Phishing Attacks
2. Ransomware Attacks
3. Loss or Theft of Equipment or Data
4. Internal, Accidental, or Intentional Data Loss
5. Attacks Against Connected Medical Devices that May Affect Patient Safety

Ten Practices

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

1. Email Protection Systems
2. Endpoint Protection Systems
3. Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Incident Response
9. Medical Device Security
10. Cybersecurity Policies

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 Cyber 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 to 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

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
Common Attributes	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
Common Attributes	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
Provider Attributes	Size (acute / post-acute)	1–25 providers	26–500 providers	Over 500 providers
Provider Attributes	Size (hospital)[15]	1–50 beds	51–299 beds	Over 300 beds
Provider Attributes	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

Main Document, p. 11

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

- Step 1 • Enumerate and Prioritize Threats
- Step 2 • Review Practices Tailored to Mitigate Threats
- Step 3 • Determine Gaps Compared to Practices
- Step 4 • Identify Improvement Opportunity and Implement
- Step 5 • Repeat for Next Threat

Resources and Templates, p. 39

Prioritize Your Threats (with Example)

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

- 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

Self-Assessment to Practices (with Example)

Cybersecurity Practices Assessment Toolkit

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*

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

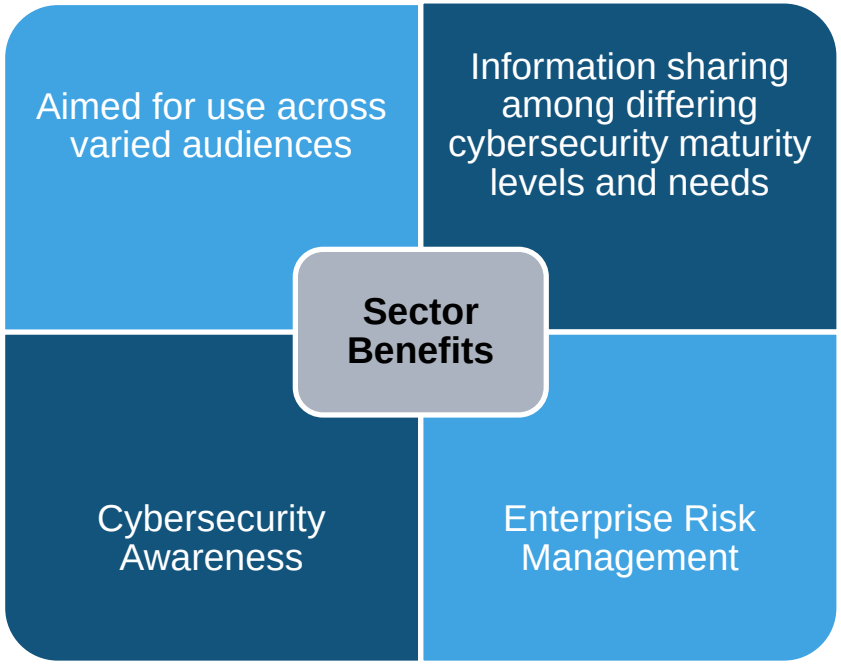
Resources and Templates, p. 41

Value and Benefits

Healthcare and Public Health (HPH) Benefits

Executives
Practitioners
InfoSec
Users

It is critical for uninterrupted care delivery and patient safety

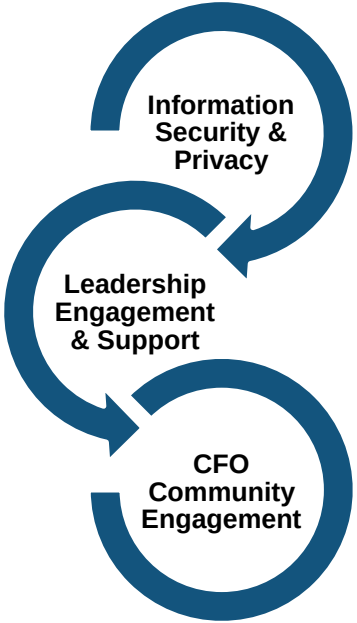


Small, medium, and large healthcare organizations can vary in their level of cybersecurity maturity and needs

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.

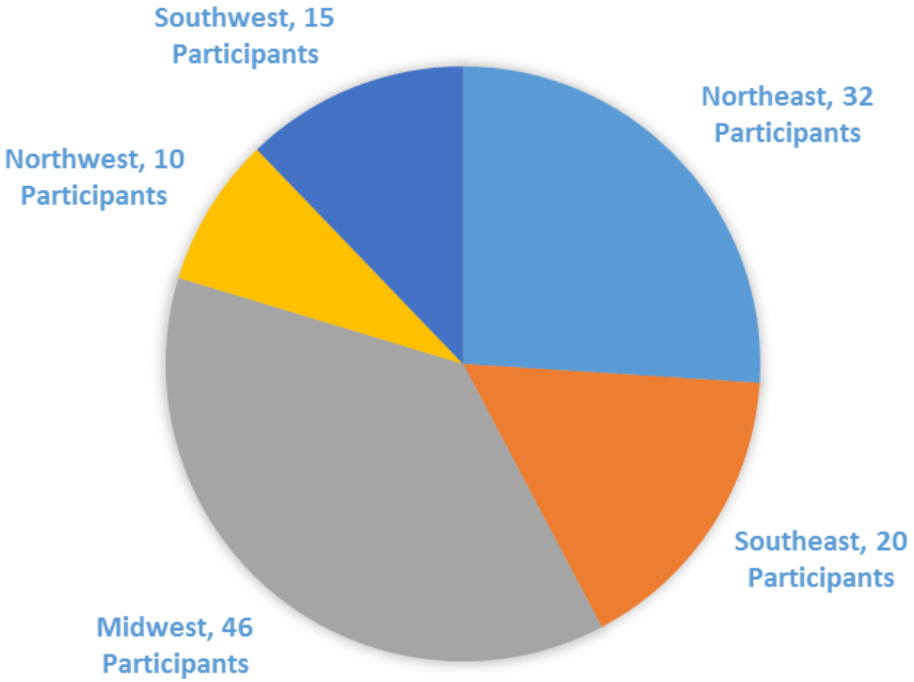
Pretesting Findings

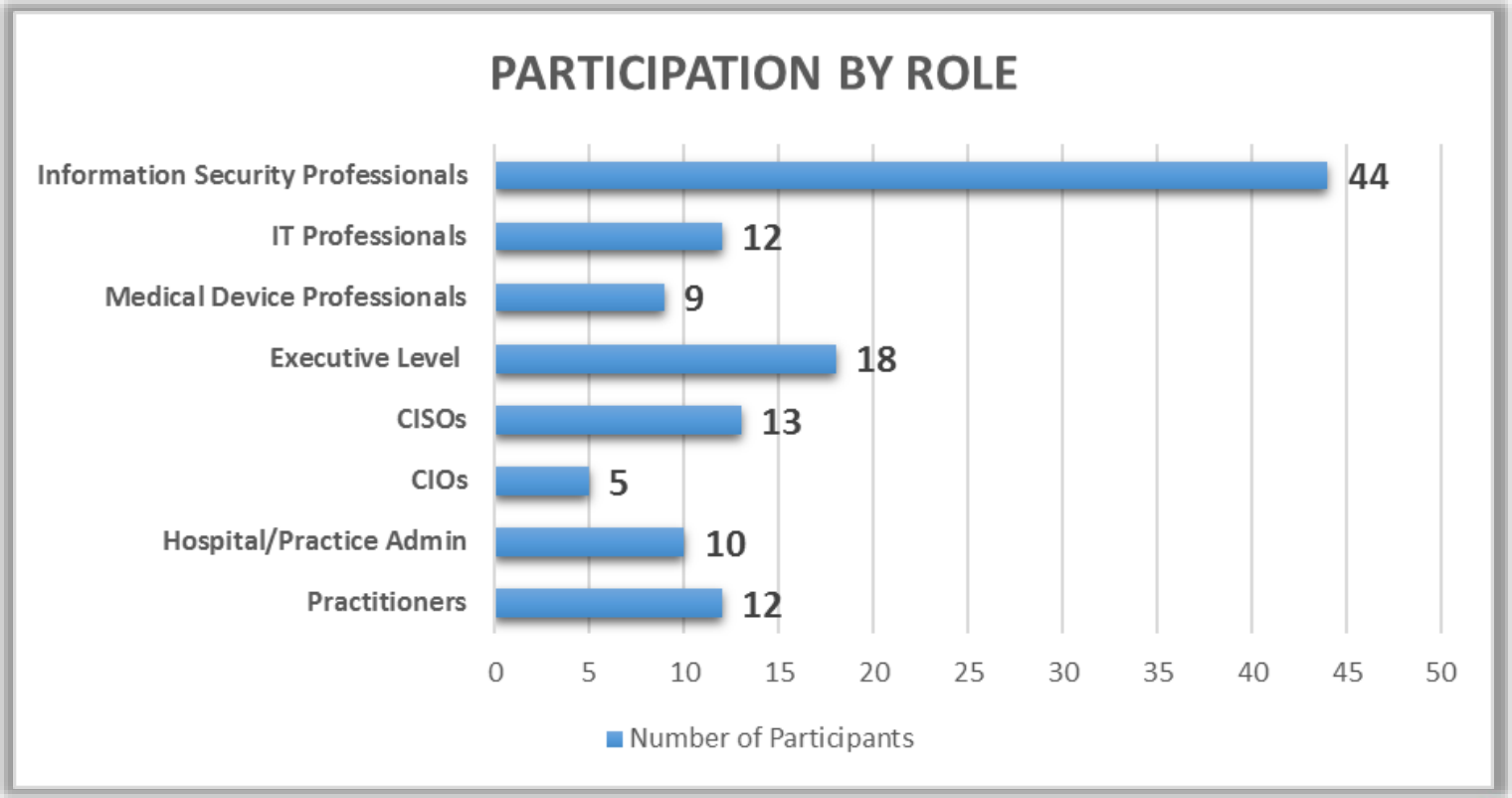
Pretesting Background

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.

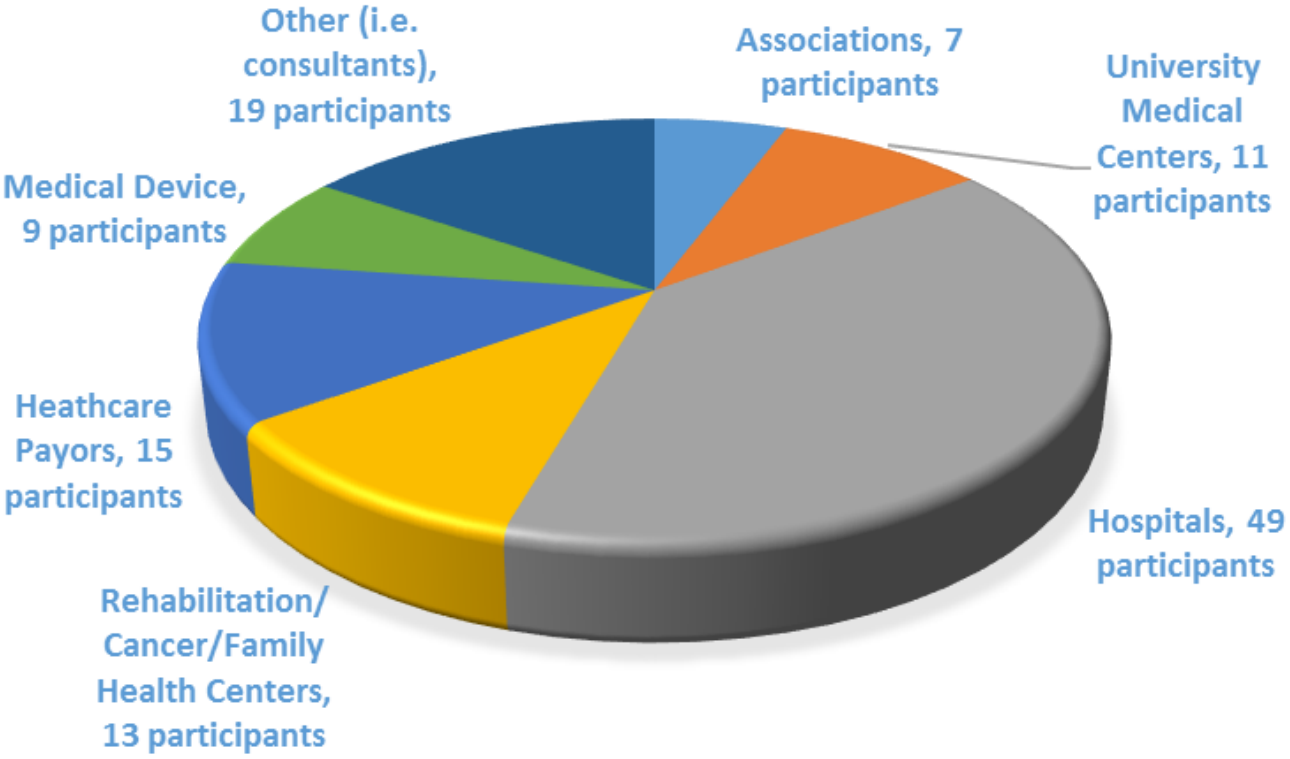
PARTICIPATION BY REGION





123 Total Participants

PARTICIPATION BY ORGANIZATION



Looking Forward & Upcoming Events

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 raise 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

HICP's Five Threats Weekly Series

Background

The HICP 5 Threats Weekly Series hosted by the 405(d) Initiative is a series of presentations focused on the 5 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-long presentations* will allow the community to dive deeper into the 5 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 5 Threats related Communication?

Visit the 405(d) Website and sign up to receive email notifications

Thank you for Joining Us

- Visit us at: www.phe.gov/405d
- Contact Us at: CISA405d@hhs.gov

Stay up to date on all things 405(d) by visiting our website!