405(d) | Aligning Healthcare Industry Security Approaches

The Cybersecurity Act of 2015

In 2015, the United States Congress passed the Cybersecurity Act of 2015 (CSA), and within this legislation is Section 405(d): Aligning Health Care Industry Security Approaches. As an approach to this requirement, in 2017 HHS convened the 405(d) Task Group leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership. The Task Group is comprised of a diverse set of over 150 members representing many areas and roles, including cybersecurity, privacy, healthcare practitioners, Health IT organizations, and other subject matter experts.

Healthcare and Public Health Sector Benefits

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

- Designed for Various Audiences
- Promotes Enterprise Risk Management
- Increases Cybersecurity Awareness
- Encourages Information Sharing

Outreach and Engagement Products

In an effort to continue to grow cybersecurity awareness across the sector we also have products and events that are available to your organization.

- The 405(d) Post Bi-Monthly Newsletter
- 405(d) Spotlight Webinar Series
- Guest Webinar Presentations
- 405(d) Cybersecurity Town Halls

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)

What is the 405(d) Program?

The 405(d) program aims to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. It seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes.

Who is Participating?

The 405(d) Task Group is convened by HHS and comprised of over 200+ information security officers, medical professionals, privacy experts, and industry leaders.

How Will the 405(d) Program Address HPH Cybersecurity Needs?

With resources and products that establish applicable & voluntary practices aimed to cost-effectively reduce the cybersecurity risks of healthcare organizations.

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in mitigating the current most pertinent cybersecurity threats to the sector.

Main Document
Examines cybersecurity threats and vulnerabilities that affect the health industry.

Technical Volume 1 & 2
Discusses ten cybersecurity practices for small, medium and large healthcare organizations

Resources and Templates Volume
Provides additional cybersecurity resources and references

The Top 5 Threats Identified in Healthcare:

- Email Phishing Attacks
- Ransomware Attacks
- Loss or Theft of Equipment or Data
- Insider, Accidental or Intentional Data Loss
- Attacks Against Connected Medical Devices That May Affect Patient Safety

10 Cybersecurity Practices

The Technical Volumes discuss these 10 practices in more detail, tailored to small, medium, and large organizations:

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

For more information on this effort and to stay up to date on all 405(d) activities, please visit the 405(d) website at www.phe.gov/405d. Or email us at CISA405d@hhs.gov

Find Us on Social Media at @ask405d

CHECK OUT OUR 405(d) RESOURCES

405(d) Spotlight Webinars

Task Group Members produce webinars with content based on real world scenarios and lessons learned, industry cybersecurity best practices, and other topics involving cybersecurity in the healthcare industry. See below for three of our most recent presentations!

- 405(d) Spotlight Webinar Featuring HC3, 405(d), DHS CISA, and H-ISAC Discussing Ransomware
- 405(d) Spotlight Featuring Greater New York Hospital Association discussing Cybersecurity Awareness at the Organization Level
- 405(d) Spotlight Webinar Featuring Medsec, New York Presbyterian Hospital, and Siemens Healthineers
- 405(d) Postlight Webinar: Staying One Step Ahead of Hackers During COVID-19

Cybersecurity Awareness Materials

The 405(d) Program has created awareness products and posters that are geared toward all levels of an organization- IT and Non IT! These items are intended to inform and educate the sector on cybersecurity tips and best practices to protect patients. See below for a few examples of our products!

- Did You Know?
- Cybersecurity Culture
- Speak Up For Patient Safety
- Cybersecurity Diet
- Have you Performed your Cybersecurity Check-Up?
- COVID 19 Clinicians and Healthcare Professionals Poster
- Teleworking Tips for the Healthcare Industry
- Are You Using New Techniques to Protect Patients?
- Is Your Organization Evolving to Protect Patients?

Task Group Cybersecurity Products

The 405(d) Task Group continues to develop Cybersecurity products that can be used for any size organization. see below for the Task Group's most recent products:

- HICP Quick Start Guide- Small Organizations
- HICP Quick Start Guide- Medium and Large Organizations
- HICP Threat Mitigation Matrix

405(d) Post

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

- 405(d) Post Volume Four- March
- 405(d) Post Volume Four- May