Cybersecurity Act of 2015
Section 405(d)
Agenda

- Purpose
- Document Overview
- Value and Benefits
- Pretesting Findings
- Next Steps
Purpose
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

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—

- (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.
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.

HOW WILL 405(d) ADDRESS HPH CYBERSECURITY NEEDS?
With a targeted set of applicable & voluntary guidance that seeks to cost-effectively reduce the cybersecurity risks of healthcare organizations.

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.

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).
Document Overview
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**
Task Group Recruitment & Management
- Identified ~110 members.
- Convened 6 times from May 2017 to March 2018

Existing Attitudes: Medical Community Baselining

Supporting the Authoring of 405(d) Guidance
- Administrative Support and Writing Counsel

Co-Authoring & Design of 405(d) Guidance
- 4 Subgroups collaboratively developed 96 page annotated outline

Assess the Output: Nationwide Pretesting

Assess the Input: Peer Review Roundtables
- 3 Focus Group Assessments
- 19 total participants including healthcare and CIOs/CISOs

Assess the Process: After Action Review
- 35 One-on-One Interviews with Task Group Members

Who Are They: Stakeholder Mapping & Analysis
- Group interviews with medical professionals and HPH CIOs/CISOs.

Version 1.0
Five Threats and Ten Practices

Assess the Process: After Action Review

Existing Attitudes: Medical Community Baselining

Version 1.0
Five Threats and Ten Practices

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

Supporting the Authoring of 405(d) Guidance
- Administrative Support and Writing Counsel

Co-Authoring & Design of 405(d) Guidance
- 4 Subgroups collaboratively developed 96 page annotated outline

Assess the Output: Nationwide Pretesting

Assess the Input: Peer Review Roundtables
- 3 Focus Group Assessments
- 19 total participants including healthcare and CIOs/CISOs

Assess the Process: After Action Review

Who Are They: Stakeholder Mapping & Analysis
- Group interviews with medical professionals and HPH CIOs/CISOs.

Version 1.0
Five Threats and Ten Practices

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

Supporting the Authoring of 405(d) Guidance
- Administrative Support and Writing Counsel

Co-Authoring & Design of 405(d) Guidance
- 4 Subgroups collaboratively developed 96 page annotated outline

Assess the Output: Nationwide Pretesting

Assess the Input: Peer Review Roundtables
- 3 Focus Group Assessments
- 19 total participants including healthcare and CIOs/CISOs

Assess the Process: After Action Review

Who Are They: Stakeholder Mapping & Analysis
- Group interviews with medical professionals and HPH CIOs/CISOs.
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
The document identifies **ten (10) practices**, which are tailored to small, medium, and large organizations and discussed in further detail in the technical volumes:

<table>
<thead>
<tr>
<th></th>
<th>Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Email Protection Systems</td>
</tr>
<tr>
<td>2</td>
<td>Endpoint Protection Systems</td>
</tr>
<tr>
<td>3</td>
<td>Access Management</td>
</tr>
<tr>
<td>4</td>
<td>Data Protection and Loss Prevention</td>
</tr>
<tr>
<td>5</td>
<td>Asset Management</td>
</tr>
<tr>
<td>6</td>
<td>Network Management</td>
</tr>
<tr>
<td>7</td>
<td>Vulnerability Management</td>
</tr>
<tr>
<td>8</td>
<td>Incident Response</td>
</tr>
<tr>
<td>9</td>
<td>Medical Device Security</td>
</tr>
<tr>
<td>10</td>
<td>Cybersecurity Policies</td>
</tr>
</tbody>
</table>
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.

- **Aimed for use across varied audiences**
- **Information sharing among differing cybersecurity maturity levels and needs**
- **Cybersecurity Awareness**
- **Enterprise Risk Management**

- **Executives**
- **Practitioners**
- **InfoSec**
- **Users**

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.

It is critical for uninterrupted care delivery and patient safety.
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 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.

**PARTICIPATION BY REGION**

- **Southwest, 15 Participants**
- **Northeast, 32 Participants**
- **Northwest, 10 Participants**
- **Southeast, 20 Participants**
- **Midwest, 46 Participants**
### Pretesting: By Role

#### Participation by Role

- Information Security Professionals: 44
- IT Professionals: 12
- Medical Device Professionals: 9
- Executive Level: 18
- CISOs: 13
- CIOs: 5
- Hospital/Practice Admin: 10
- Practitioners: 12

*Total Participants: 123*
Pretesting: By Organization

**PARTICIPATION BY ORGANIZATION**

- **Medical Device, 9 participants**
- **Medical Device, 9 participants**
- **Healthcare Payors, 15 participants**
- **Rehabilitation/Cancer/Family Health Centers, 13 participants**
- **Associations, 7 participants**
- **University Medical Centers, 11 participants**
- **Other (i.e. consultants), 19 participants**
- **Hospitals, 49 participants**
Next Steps
405(d) Stages*

Stage One: “Foundation”
- May 22-23 2017: Session #1 (In-Person)
- June 26 2017: Session #2 (WebEx)
- July 17-18 2017: Session #3 (In-Person)

Stage Two: “How-To”/Subgroups
- August 2017 – Early September 2017: Subgroups Convene and Address “Annotated Outline” and Topics

Stage Three: “Assessment”
- September 18-19: Session #4 (In-Person)

Stage Four: “Initial Document”

Stage Five: “Pre-Testing”
- Summer 2018 – Fall 2018: Assessing the Output: Nationwide Pre-Testing with Healthcare Professionals

• Next Stages || Sustained Engagement: Winter-2018: Release to Industry; Informing and Educating; Moving to V2.0

* Dates Subject to Change