Conflict of Interest

Andrea Arbelaez, has no real or apparent conflicts of interest to report.

Sue Wang, has no real or apparent conflicts of interest to report.
Agenda

• A healthcare journey and cyber risks – use of Picture Archiving and Communication System (PACS)

• Overview of National Cybersecurity Center of Excellence (NCCoE)

• Deep Dive into NCCoE PACS project

• Summary of NCCoE Healthcare portfolio

• Conclusion
Learning Objectives

• Demonstrate how healthcare delivery organizations can secure their PACS

• Evaluate risks associated with threats and vulnerabilities related to the PACS and the vast assortment of readily available commercial technologies that can be employed to mitigate risks

• Manage applied knowledge of how to implement similar security controls in existing HDO ecosystems

• Discuss the NIST Cybersecurity Framework and medical device standards incorporated in the PACS Project
A healthcare journey
PACS: Picture Archiving and Communications System
Risks of unsecured PACS

Confidentiality
• Fraudulent use of health insurance information
• Identity theft and fraudulent use of PHI
• Patient personal distress due to disclosure

Integrity
• Patient diagnoses disrupted or delayed; leading to patient safety concerns

Availability
• Ransomware attack leading to process disruptions
• PACS vulnerabilities serve as pivot point for attacks elsewhere on enterprise network
National Cybersecurity Center of Excellence
NCCoE Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs
Collaborative Hub

• The NCCoE works on critical national problems in cybersecurity.
• The NCCoE has access to a wealth of expertise, resources, relationships, and experience.
NCCoE Tenets

Standards-based
Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

Modular
Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable
Provide a detailed practice guide including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

Commercially available
Work with the technology community to identify commercially available products that can be brought together in example solutions to address challenges identified by industry

Usable
Design blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent
Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications
Engagement & Business Model

**DEFINE**
- OUTCOME: Define a scope of work with industry to solve a pressing cybersecurity challenge

**ASSEMBLE**
- OUTCOME: Assemble teams of industry orgs, govt. agencies, and academic institutions to address all aspects of the cybersecurity challenge

**BUILD**
- OUTCOME: Build a practical, usable, repeatable implementation to address the cybersecurity challenge

**ADVOCATE**
- OUTCOME: Advocate adoption of the example implementation using the practice guide
SP 1800 Series: Cybersecurity Practice Guides

Volume A: Executive Summary

- High-level overview of the project, including summaries of the challenge, solution, and benefits

Volume B: Approach, Architecture, and Security Characteristics

- Deep dive into challenge and solution, including approach, architecture, and security mapping to NIST Cybersecurity Framework and other relevant standards

Volume C: How-To Guide

- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance
Securing Picture Archiving and Communications System (PACS)
Why did we select PACS?

Connected Medical Devices Deployed

- Infusion Pump: 48%
- Imaging System: 18.70%
- Patient Monitor: 17.20%
- Point of Care Analyzer: 6.60%
- Medical Device Gateway: 4.40%
- ECG Machine: 1.90%
- Patient Tracking: 1.30%
- Nurse Call System: 1.10%
- Other Healthcare: 0.40%
- Medical Printer: 0.30%

Source: ZingBox, "Threat Report on IOT Medical Devices", 1/25/18
Why did we select PACS?

Source: ZingBox, “Threat Report on IOT Medical Devices”, 1/25/18
Approach to PACS Cybersecurity Practice Guide

1. Define Interactions between PACS and network systems
2. Identify Security Risks
3. Review Security Technologies and Standards
4. Build example implementation to address cybersecurity challenge
5. Publish NIST SP 1800 series document

Identify Security Risks

Define Interactions between PACS and network systems

Review Security Technologies and Standards

Build example implementation to address cybersecurity challenge

Publish NIST SP 1800 series document
NCCoE PACS Build Team

- Cisco
- Clearwater Compliance
- Digicert
- Forescout
- Hyland
- Iron Mountain
- Philips Healthcare
- Symantec
- TDI Technologies
- Tempered Networks
- Tripwire
- Virta Labs
- Zingbox
Where do we begin?

Security controls will not always work as expected, and may contain vulnerabilities.

Other technology deployed in the environment will have vulnerabilities.

Patches and updates won’t be made available at the same rate as weaknesses are identified.

HIT will have vulnerabilities.
Security controls will not always work as expected, and may contain vulnerabilities.

Other technology deployed in the environment will have vulnerabilities.

Patches and updates won’t be made available at the same rate as weaknesses are identified.

HIT will have vulnerabilities.

Ensure your infrastructure has protective and detective controls.

Segregate your environment.

Use multiple controls to enforce your segregation – no single points of failure!

Verify if you’re using latest version.
Cybersecurity Standards and Guidance

**NIST**
- Cybersecurity Framework
- Risk Management Framework (RMF)
- SP 800-53: Security Controls

**FDA**
- Cybersecurity Premarket Guidance
- Cybersecurity Postmarket Guidance

**ISO/IEC 80001:** Application of Risk Management for IT Networks Incorporating Medical Devices

**IHE:** Medical Device Cyber Security - Best Practice Guide

**AAMI TIR57:** Principles for Medical Device Security - Risk management
### Using NIST Cybersecurity Framework

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td>ID.BE</td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td>ID.GV</td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td>ID.RA</td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>ID.RM</td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.RA1</td>
<td>Risk Assessment (ID.RA)</td>
</tr>
</tbody>
</table>

#### Cybersecurity Framework (CSF) v1.1

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>SPR000-5318A</th>
<th>Sector-Specific Standards &amp; Best Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>DE</td>
<td>Detect</td>
<td>PR.DS-1: Data Breach is detected</td>
<td>ISAGU, STCF, HIPAA Security Rule 45, ISO/IEC 27002</td>
<td></td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>DETECT [DE]</td>
<td>ISAGU, STCF, HIPAA Security Rule 45, ISO/IEC 27002</td>
<td></td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>ISAGU, STCF, HIPAA Security Rule 45, ISO/IEC 27002</td>
<td></td>
</tr>
</tbody>
</table>

23
Securing Picture Archiving and Communications System (PACS)

Project Status
Build Phase - Working with technology collaborators in the NCCoE lab to develop reference designs and draft practice guides

Collaborate with Us
• Read Securing PACS Project Description
• Email HIT_nccoec@nist.gov to join the Community of Interest for this project
PACS Project Schedule

2018

Q2
FRN publication (9. May)

Q3
Collaborators sign CRADA

Q4
Build Reference Architecture and write Practice Guide (NIST 1800-series)

Publish Draft Practice Guide

2019

Build Team finalized
NCCoE Portfolio

- Attribute Based Access Control (SP 1800-3)
- Consumer/Retail: Multifactor Authentication for e-Commerce
- Data Integrity: Identifying and Protecting
- Data Integrity: Detecting and Responding
- Data Integrity: Recovering (SP 1800-11)
- Derived PIV Credentials (SP 1800-12)
- DNS-Based Email Security (SP 1800-6)
- Energy: Identity and Access Management (SP 1800-2)
- Energy: Situational Awareness (SP 1800-7)
- Financial Services: Access Rights Management (SP 1800-9)
- Financial Services: IT Asset Management (SP 1800-5)
- Healthcare: Securing Electronic Health Records on Mobile Devices (SP 1800-1)
- Healthcare: Securing Wireless Infusion Pumps (SP 1800-8)
- Healthcare: Securing Picture Archiving and Communication Systems (PACS)
- Healthcare: Securing Telehealth Remote Patient Monitoring Ecosystem
- Hospitality: Securing Property Management Systems
- Mitigating IoT-Based DDoS
- Manufacturing: Capabilities Assessment for Securing Manufacturing Industrial Control Systems
- Mobile Device Security: Cloud and Hybrid Builds (SP 1800-4)
- Mobile Device Security: Enterprise Builds
- Mobile Threat Catalogue
- Privacy-Enhanced Identity Federation
- Public Safety/First Responder: Mobile Application SSO
- Secure Inter-Domain Routing
- TLS Server Certificate Mgmt
- Transportation: Maritime: Oil & Natural Gas
- Trusted Geolocation in the Cloud (NISTIR 7904)
NIST SP 1800-1: Securing Electronic Health Records on Mobile Devices

Project Status

**Advocate Stage** – Final guide published in August 2018

Collaborate with Us

- Read [Securing EHR Practice Guide](#)
- Email [HIT_nccoe@nist.gov](mailto:HIT_nccoe@nist.gov) to join the Community of Interest for this project
NIST SP 1800-1: Securing Electronic Health Records on Mobile Devices
NIST SP 1800-8: Securing Wireless Infusion Pumps

Project Status

**Advocate Stage** – Final guide published in August 2018

Collaborate with Us

- Read SP 1800-8: [Securing Wireless Infusion Pumps](#)
- Email [HIT_ncco@nist.gov](mailto:HIT_ncco@nist.gov) to join the Community of Interest for this project
NIST SP 1800-8: Securing Wireless Infusion Pumps
Securing Telehealth Remote Patient Monitoring Ecosystem
Securing Telehealth Remote Patient Monitoring Ecosystem

Project Status

Define Phase – Seeking public comments on draft Project Description. Comment period closed on December 21, 2018

Collaborate with Us

- Read Securing Telehealth RPM Project Description
- Email HIT_nccoe@nist.gov to join the Community of Interest for this project
Securing Telehealth Remote Patient Monitoring Ecosystem
Summary of Learning Objectives

Here’s what we covered:

• A high-level depiction of the PACS ecosystem
• Some cyber risks facing healthcare technology
• An introduction to some standards and frameworks as they apply to cyber health
• Discussion of an implementation of cyber controls
• Use NCCoE as your resource and collaborate with us to help you and others for improving cybersecurity in healthcare!
Ways to Collaborate

Contact the NCCoE Healthcare Project Team
HIT_nccoe@nist.gov
301-975-0200

To Collaborate, visit:
nccoe.nist.gov/healthcare
Questions

Andrea Arbelaez, Healthcare IT Project Manager, NIST
Sue Wang, Cybersecurity Engineer, MITRE Corp.

Contact us:
HIT_nccoe@nist.gov
301-975-0200