National Cybersecurity Center of Excellence

Increasing the adoption of standards-based cybersecurity technologies

Hospitality Sector Project

NIST SP 1800-27 Securing Property Management Systems

Bill Newhouse, Cybersecurity Engineer

May 20, 2021

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

National Institute of Standards and Technology

Mission: To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Information Technology Laboratory

Applied Cybersecurity Division

Other NIST Laboratories
Communications Technology Laboratory
Engineering Laboratory
Material Measurement Laboratory
Physical Measurement Laboratory

User Facilities
NIST Center for Neutron Research
Center for Nanoscale Technologies (NanoFab)

Other ITL Divisions
Advanced Network Technologies Division
Computer Security Division
Information Access Division
Software and Systems Division
Applied and Computational Mathematics Division
Statistical Engineering Division

https://nist.gov/cybersecurity

Cybersecurity & Privacy @ NIST | 9 Priority Areas

Learn more:
nist.gov/blogs/cybersecurity-insights/2021-whats-ahead-nist-cybersecurity-and-privacy

Identity & Access Management

Trustworthy Platforms

Securing Emerging Technologies

Trustworthy Networks

Awareness, Training, Education & Workforce Development

Metrics & Measurement

Privacy

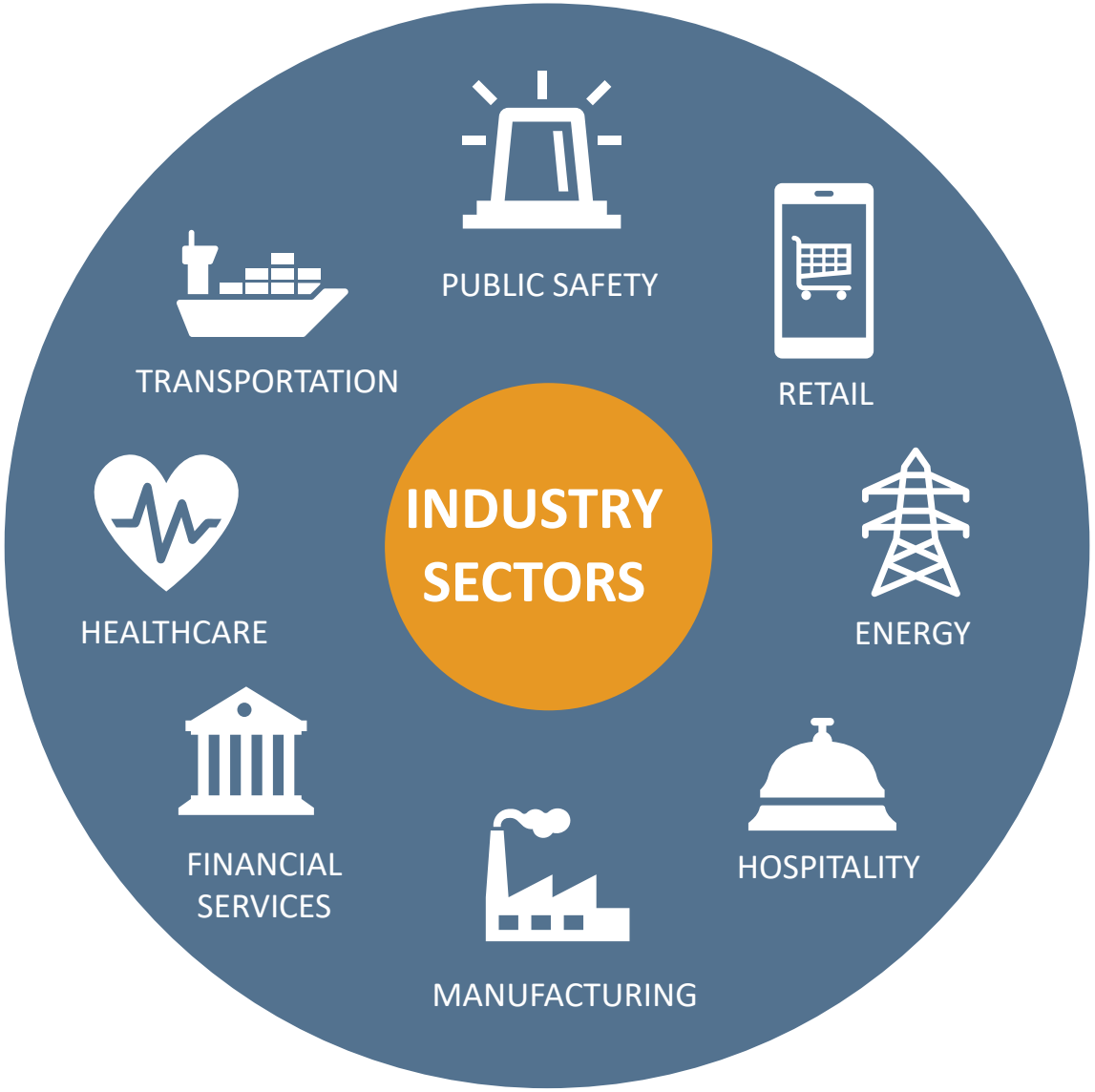
Strengthening Cryptographic Standards & Validation

Enhancing Risk Management

National Cybersecurity Center of Excellence Mission

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

Securing industry Sectors



- Commerce/Retail
- Energy
- Financial Services
- Healthcare
- Hospitality
- Manufacturing
- Public Safety/First Responder
- Transportation

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 detailed guidance 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

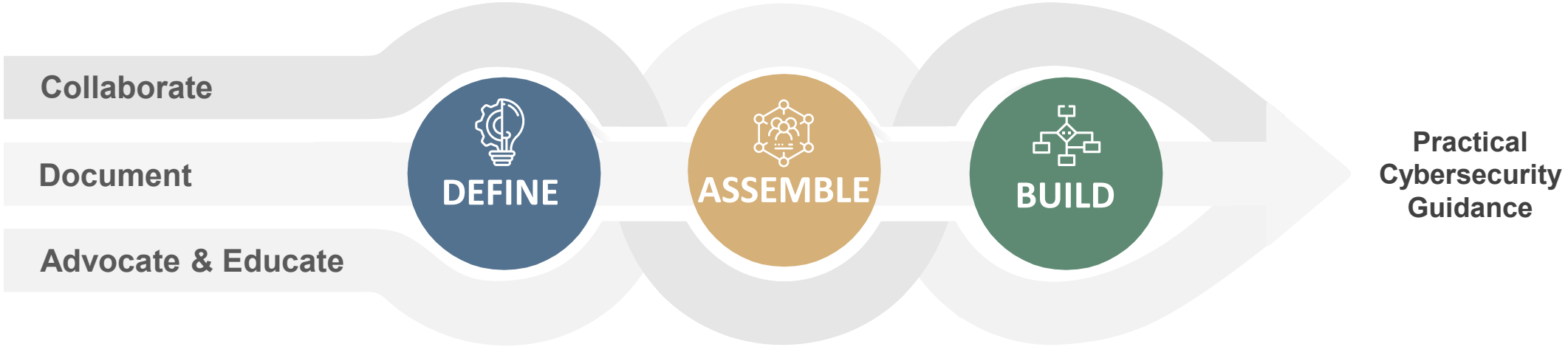
Usable

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

OUR APPROACH

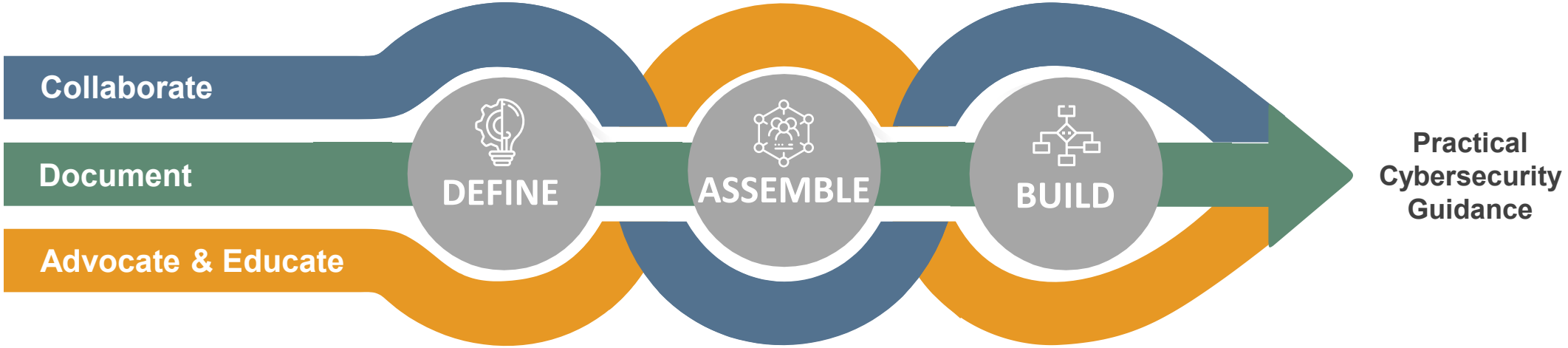


Define a scope of work with industry to solve a pressing cybersecurity challenge

Assemble teams to address all aspects of the cybersecurity challenge

Build a practical, usable, repeatable implementation to address the cybersecurity challenge

OUR APPROACH



Define a scope of work with industry to solve a pressing cybersecurity challenge

Assemble teams to address all aspects of the cybersecurity challenge

Build a practical, usable, repeatable implementation to address the cybersecurity challenge

NCCoE Cross-Sector Projects

- Attribute Based Access Control (SP 1800-3)
- Data Integrity (SP 1800-11)
- Derived PIV Credentials (SP 1800-12)
- DNS-Based Secured Email (SP 1800-6)
- Mitigating IoT-Based DDoS (SP 1800-15)
- Mobile Device Security (SP 1800-4 & SP 1800-21)
- Secure Inter-Domain Routing (SP 1800-14)
- TLS Server Certificate Management (SP 1800-16)
- Trusted Geolocation in the Cloud (SP 1800-19)

https://www.nccoe.nist.gov/projects

Recent Publications

- DRAFT Securing the Internet of Things, Securing the Industrial Internet of Things: Cybersecurity for the Distributed Energy Resources (NIST Special Publication (SP) 1800-32)
- DRAFT Establishing Confidence in IoT Device Security: How do we get there (white paper)
- Cybersecurity and Privacy International Engagement Updates (Cybersecurity Blog)
- DRAFT Mobile Device Security: Bring Your Own Device (SP 1800-22)
- 2nd DRAFT Securing Telehealth Remote Patient Monitoring Ecosystem (SP 1800-30)
- Challenges with Adopting Post-Quantum Cryptographic Algorithms (Final Report)
- **Securing Property Management Systems** (SP 1800-27)

WHY FOCUS ON PROPERTY MANAGEMENT SYSTEMS?

- Hospitality organizations rely on a Property Management System (PMS) for daily tasks, planning, and record keeping.

- A PMS interfaces with several services and components within a hotel's IT systems, such as point-of-sale (POS) systems, physical access control systems, Wi-Fi networks, and other employee and guest service applications.

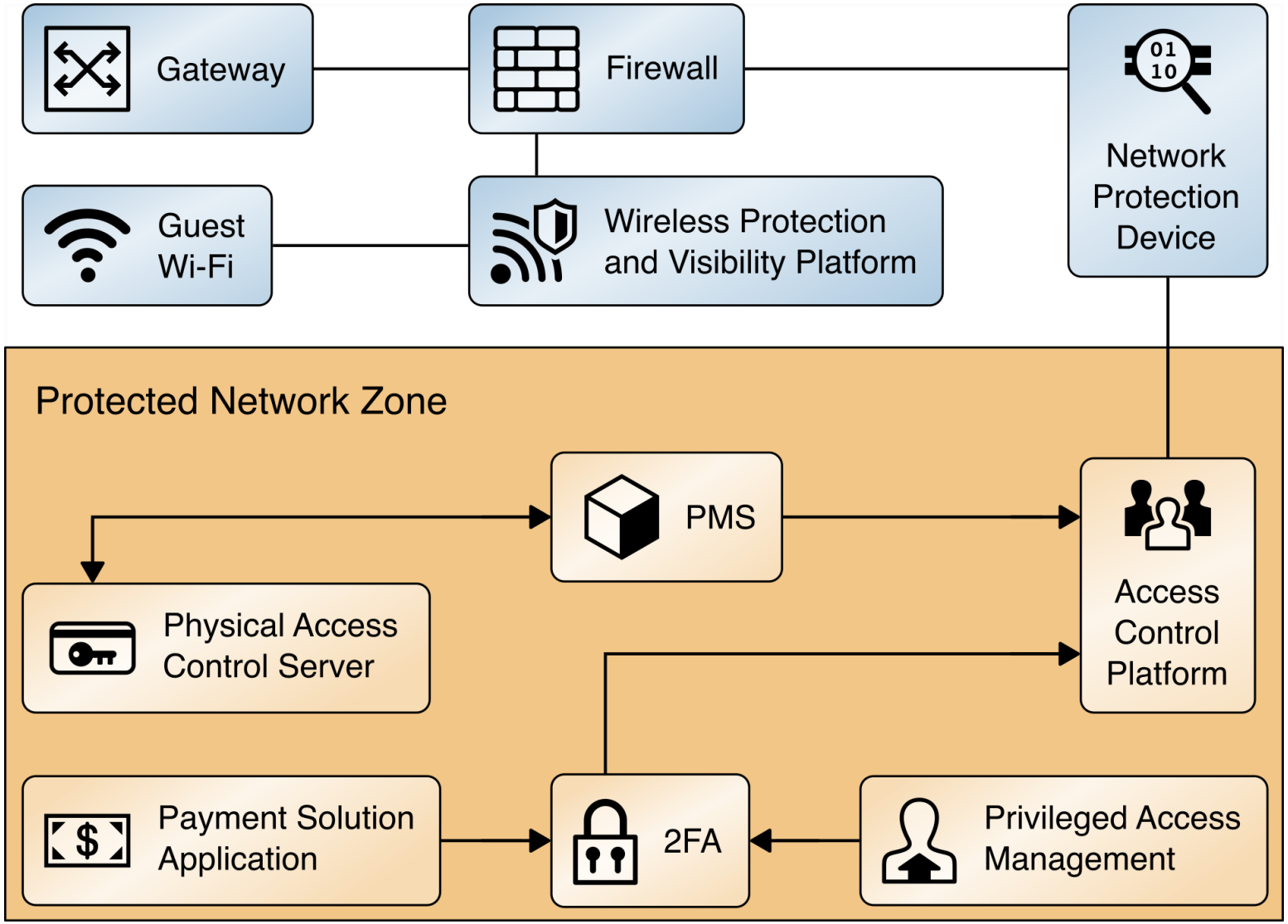
- Store, process, and transmit a variety of sensitive guest information, including payment card information (PCI) and personally identifiable information (PII).

- An unsecured or poorly secured PMS could allow a data breach or denial of service disruptions.

DESIGNED TO HELP ORGANIZATIONS

- Increase overall PMS security situational awareness, and limit exposure of the PMS to incidents in systems that interface with it.
- Control and limit access to your PMS to those with a business need.
- Instill consumer confidence and brand loyalty by protecting guest privacy and payment card information.
- Decrease breach potential and data exfiltration by limiting lateral movement, thus decreasing organizational risk.
- Build the business case, functional requirements, and test plan for a similar solution within your own environment.
- Support privacy/regulatory compliance by using data tokenization and limiting the spread of data beyond “need-to-know.”

HIGH LEVEL ARCHITECTURE



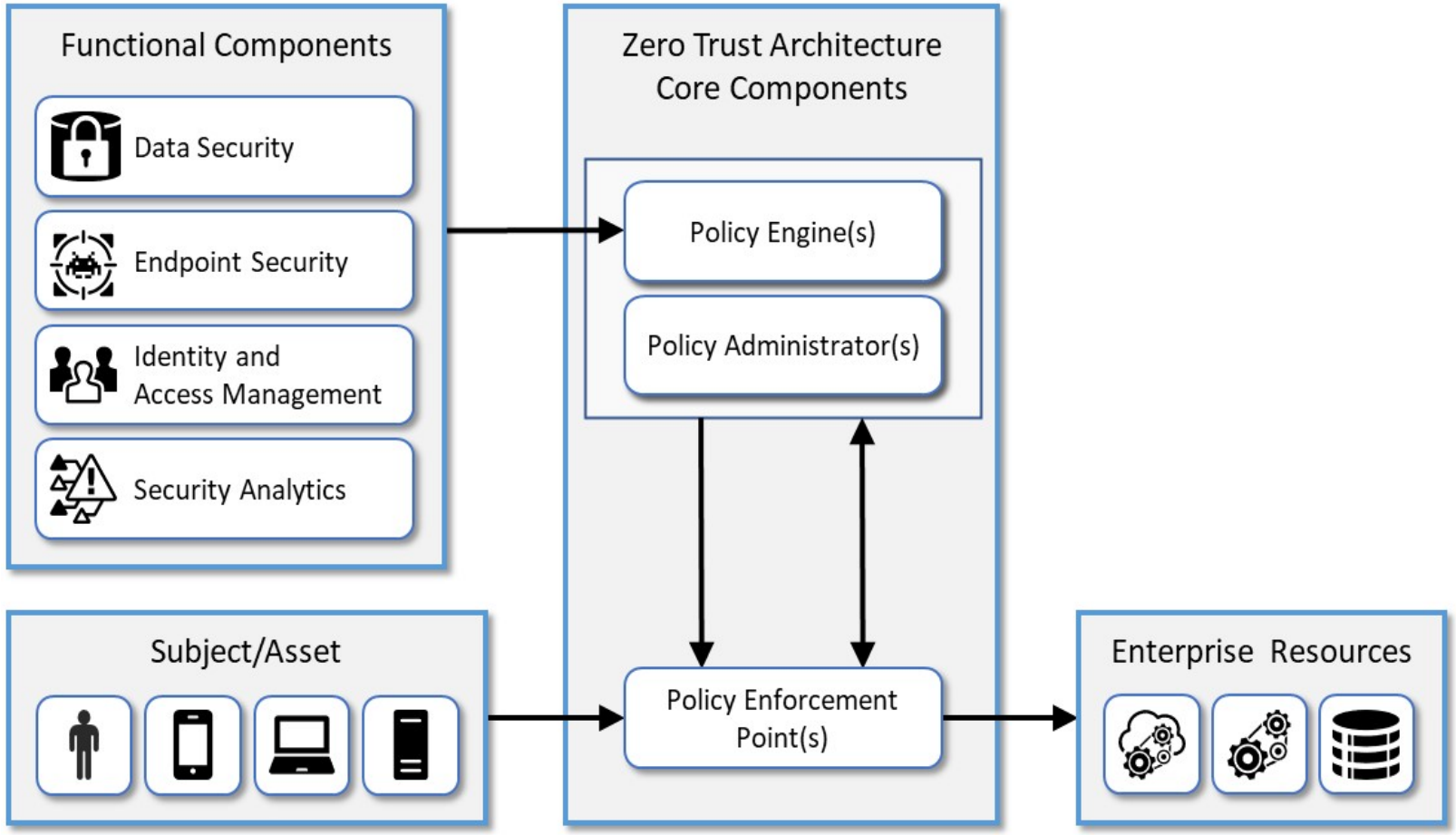
FRAMING RISK USING THE NIST CYBERSECURITY FRAMEWORK

NIST Cybersecurity Framework v1.1			Standards and Best Practices		
Function	**Category**	**Subcategory**	**PCI DSS v3.2.1**	**NIST SP 800-53r5 Security and Privacy Controls [9]**	**NICE Framework 2017 Work Roles [11]**
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and man-	**ID.AM-1:** Physical devices and systems within the organization are inventoried.		CM-8, PM-5	Technical Support Specialist
		ID.AM-2: Software platforms and applications within the organization are inventoried.		CM-8, PM-5	Technical Support Specialist

ZERO TRUST ARCHITECTURE

Zero Trust Tenet	PMS reference design Component	Cybersecurity Framework Subcategories
All data sources and computing services are considered resources.	CryptoniteNXT Secure Zone 2.9.1	**ID.AM-1** Physical devices and systems within the organization are inventoried. **ID.AM-2** Software platforms and applications within the organization are inventoried.
All communication is secured regardless of network location; network location does not imply trust.	CryptoniteNXT Secure Zone 2.9.1 StrongKey's vault	**PR.AC-5** Network integrity is protected. **PR.DS-1** Data at-rest is protected **PR.DS-2** Data in transit is protected. **PR.PT-4** Communications and control networks are protected.
Access to individual enterprise resources is granted on a per-session basis; trust in the requester is evaluated before the access is granted.	TDi ConsoleWorks 5.2-0u1	**PR.AC-1** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes. **PR.PT-3** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.

ZERO TRUST ARCHITECTURE COMPONENTS



ZERO TRUST ARCHITECTURE COMPONENTS TABLE

PMS Reference Design Component	Zero Trust Component
pfSense Firewall	Endpoint Security
TDi ConsoleWorks	Identity and Access Management (IDAM)
Remediant SecureOne	Security Analytics
Data encryption at rest (in StrongKey StrongAuth KeyAppliance and Solidres PMS) and in transit	Data Security
CryptoniteNXT Administration Control Center (ACC)	Policy Engine
Domain users with access permission to the CryptoniteNXT administrator workstation	Policy Administrators
Any device within the CryptoniteNXT Secure Zone, including PMS and other security components	Policy Enforcement Points
User	Asset
Workstation	Asset
Solidres PMS	Enterprise Resource
Data in Solidres PMS	Enterprise Resource
StrongKey StrongAuth KeyAppliance vault	Enterprise Resource
Credit Card data in StrongKey StrongAuth KeyAppliance vault	Enterprise Resource

NIST PRIVACY FRAMEWORK

The NIST Privacy Framework was published after we began to build our property management system reference design.

- We included a short section in Volume B of our practice guide to draw attention to the Privacy Framework.

- Protecting an individual's privacy should become a core value for PMS designs through more thorough use of the Privacy Framework.

- The NIST Privacy Framework Core provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk.

- The Privacy Framework Function, Category, and Subcategory are mapped to the component in the PMS reference design most impactful on achieving the subcategory outcome.

NIST PRIVACY FRAMEWORK TABLE

Privacy Framework Function	Privacy Framework Category	Privacy Framework Subcategory	PMS reference design Component
Identify-P	Inventory and Mapping (ID.IM-P)	**ID.IM-P4:** Data actions of the systems/products/services are inventoried.	Forescout CounterACT 8.1
		ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components, roles of the component owners/operators, and interactions of individuals or third parties with the systems/products/services.	CryptoniteNXT Secure Zone 2.9.1 StrongKey KeyAppliance
Control-P	Data Processing Management (CT.DM-P)	**CT.DM-P1:** Data elements can be accessed for review.	Solidres PMS Forescout CounterACT 8.1
		CT.DM-P2: Data elements can be accessed for transmission or disclosure.	Solidres PMS
		CT.DM-P3: Data elements can be accessed for alteration.	Solidres PMS

Bill Newhouse

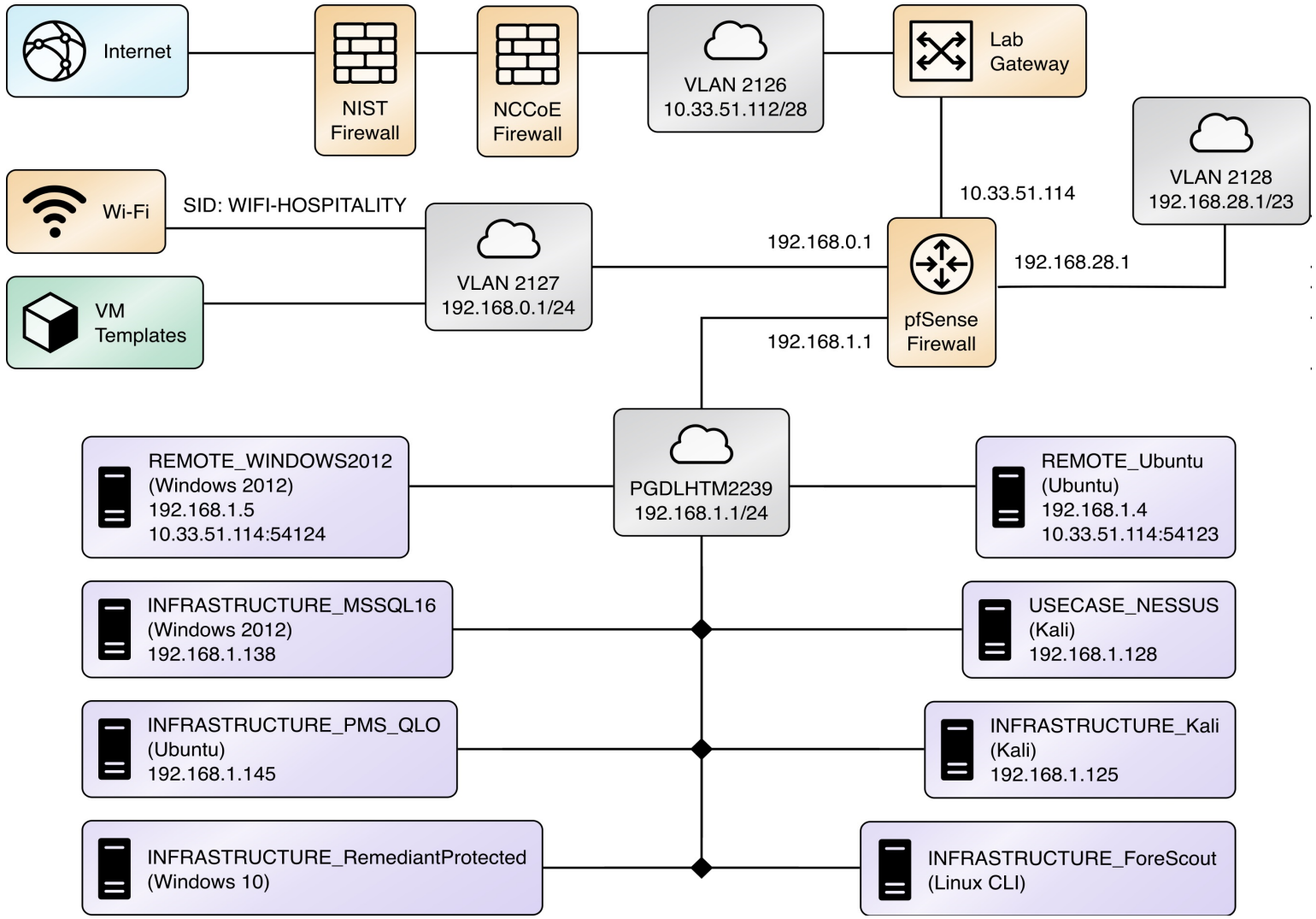
william.newhouse@nist.gov

@cybernewhouse

nccoe.nist.gov

@NISTcyber

DETAILED ARCHITECTURE (1 OF 2)



DETAILED ARCHITECTURE (2 OF 2)