

NCCoE Supply Chain Assurance Project

National Cybersecurity Center of Excellence

Industry Day
9/10/2019



Emergency Procedures for NCCoE Visitors

Evacuation Emergencies

What is an Evacuation Emergency?

- Fires
- Explosions
- Earthquakes
- Indoor toxic material releases
- Indoor radiological and biological accidents
- Workplace violence

What Will Happen During an Evacuation Event?

- A building-wide alarm will sound
- Verbal instructions over the building's public address (PA) system will follow shortly after the alarm
- Exit the conference room and head for the nearest exit (**Red Signs – Upper Right Map**)
- If the Security Guard is close by and accessible, ask for further instruction
- Once outside the building, swiftly walk toward the designated meeting area near the posted sign stating "Evacuation Meeting Area" (**Yellow Sign – Lower Right Map**)

Shelter-In-Place (SIP) Emergencies

What is a Shelter-In-Place Emergency?

- Severe weather (hurricanes, tornadoes, etc.)
- chemical, biological, or radiological contaminants released into the environment

What Will Happen During an Evacuation Event?

- A building-wide alarm will sound
- Verbal instructions over the building's public address (PA) system will follow shortly after the alarm
- Exit the conference room and head for the nearest SIP hallway or room (**Yellow Signs – Upper Right Map**)
- If the Security Guard is close by and accessible, ask for further instruction



> Agenda

- 9:00-9:15: Safety Brief/Intro to NCCoE**
- 9:15-9:30: Cyber Supply Chain Risk Management Overview**
- 9:30-9:45: Project Description Overview**
- 9:45-9:55: Trusted Computing Architecture**
- 9:55-10:10: Break**
- 10:10-11:35: Industry Session**
- 11:35-12:05: Industry Panel Q&A**
- 12:05-12:30: Wrap-Up**



National Institute of Standards and Technology



> National Institute of Standards and Technology



NIST is a bureau under the Department of Commerce. NIST's mission is 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.

NIST runs a number of laboratories to assist in its mission.

Communications
Technology
Laboratory

Engineering
Laboratory

Information
Technology
Laboratory

Material
Measurement
Laboratory

Physical
Measurement
Laboratory



Introduction to NCCoE





Introduction to NCCoE



> NCCoE Mission

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



> Engagement & Business Model

DEFINE



ASSEMBLE



BUILD



ADVOCATE



OUTCOME:

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



OUTCOME:

Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge



OUTCOME:

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



OUTCOME:

Advocate adoption of the example implementation using the practice guide

> 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

> 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 the 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

| CSF Function | CSF Subcategory | SP800-53R4 ^a | IEC/ISO 27001 ^b | CIS CSC ^c | NERC-CIP v5 ^d |
|--------------|--|--|--|----------------------|--------------------------|
| Identify | ID.AM-1: Physical devices and systems within the organization are inventoried | CM-8 | A.8.1.1 A.8.1.2 | CSC-1 | CIP-002-5.1 |
| | ID.AM-2: Software platforms and applications within the organization are inventoried | CM-8 | A.8.1.1 A.8.1.2 | CSC-2 | CIP-002-5.1 |
| Protect | PR.AC-2: Physical access to assets is managed and protected | PE-2, PE-3, PE-4, PE-5, PE-6, PE-9 | A.11.1.1 A.11.1.2 A.11.1.4 A.11.1.6 A.11.2.3 | | CIP-006-6 |
| | PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity | SI-7 | A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3 | | |
| Detect | DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed | AC-4, CA-3, CM-2, SI-4 | | | |
| | DE.AE-2: Detected events are analyzed to understand attack targets and methods | AU-6, CA-7, IR-4, SI-4 | A.16.1.1 A.16.1.4 | | CIP-008-5 |
| | DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors | AU-6, CA-7, IR-4, IR-5, IR-8, SI-4 | | | CIP-007-6 |

> Sector-Based Projects



Commerce/Retail (SP 1800-17)

Energy (SP 1800-2 & SP 1800-7)

Financial Services (SP 1800-5 & SP 1800-9
& SP 1800-18)

Healthcare (SP 1800-1 & SP 1800-8)

Hospitality

Manufacturing

Public Safety/First Responder (SP 1800-13)

Transportation

> 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)



Overview of NIST's Cyber Supply Chain Risk Management (C-SCRM) Program



From *The World Is Flat* by Thomas Friedman

Dell Inspiron 600m Notebook: Key Components and Suppliers

| Component | Supplier or Potential Suppliers |
|------------------------|--|
| Intel Microprocessor |  US-owned factory in the Philippines, Costa Rica, Malaysia, or China (<i>Intel</i>) |
| Memory |  South Korea (<i>Samsung</i>), Taiwan (<i>Nanya</i>), Germany (<i>Infineon</i>), or Japan (<i>Elpida</i>) |
| Graphics Card |  China (<i>Foxconn</i>), or Taiwanese-owned factory in China (<i>MSI</i>) |
| Cooling fan |  Taiwan (<i>CCI and Auras</i>) |
| Motherboard |  Taiwan (<i>Compal and Wistron</i>), Taiwanese-owned factory in China (<i>Quanta</i>), or South Korean-owned factory in China (<i>Samsung</i>) |
| Keyboard |  Japanese company in China (<i>Alps</i>), or Taiwanese-owned factory in China (<i>Sunrex and Darfon</i>) |
| LCD |  South Korea (<i>Samsung, LG.Philips LCD</i>), Japan (<i>Toshiba or Sharp</i>), or Taiwan (<i>Chi Mei Optoelectronics, Hannstar Display, or AU Optronics</i>) |
| Wireless Card |  Taiwan (<i>Askey or Gemtek</i>), American-owned factory in China (<i>Agere</i>) or Malaysia (<i>Arrow</i>), or Taiwanese-owned factory in China (<i>USI</i>) |
| Modem |  China (<i>Foxconn</i>), or Taiwanese company in China (<i>Asustek or Liteon</i>) |
| Battery |  American-owned factory in Malaysia (<i>Motorola</i>), Japanese company in Mexico, Malaysia, or China (<i>Sanyo</i>), or South Korean or Taiwanese factory (<i>SDI and Simplo</i>) |
| Hard Disk Drive |  American-owned factory in Singapore (<i>Seagate</i>), Japanese-owned company in Thailand (<i>Hitachi or Fujitsu</i>), or Japanese-owned company in the Philippines (<i>Toshiba</i>) |
| CD/DVD |  South Korean company with factories in Indonesia and Philippines (<i>Samsung</i>), Japanese-owned factory in China or Malaysia (<i>NEC</i>), Japanese-owned factory in Indonesia, China, or Malaysia (<i>Teac</i>), or Japanese-owned factory in China (<i>Sony</i>) |
| Notebook Carrying Bag |  Irish company in China (<i>Tenba</i>), or American company in China (<i>Targus, Samsonite, and Pacific Design</i>) |
| Power Adapter |  Thailand (<i>Delta</i>), or Taiwanese-, South Korean-, or American-owned factory in China (<i>Liteon, Samsung, and Mobility</i>) |
| Power Cord |  British company with factories in China, Malaysia, and India (<i>Voalex</i>) |
| Removable Memory Stick |  Israel (<i>M-System</i>), or American company with factory in Malaysia (<i>Smart Modular</i>) |

> C-SCRM Defined

- Risks **TO** and **THROUGH** the supply chain
- People, Processes, & Technologies
- Reduce **vulnerability, threat, and/or impact**
- **Overlaps but is not strictly:**
 - Cybersecurity
 - Supply chain management
 - Quality management
 - Third-party risk management
 - Etc.

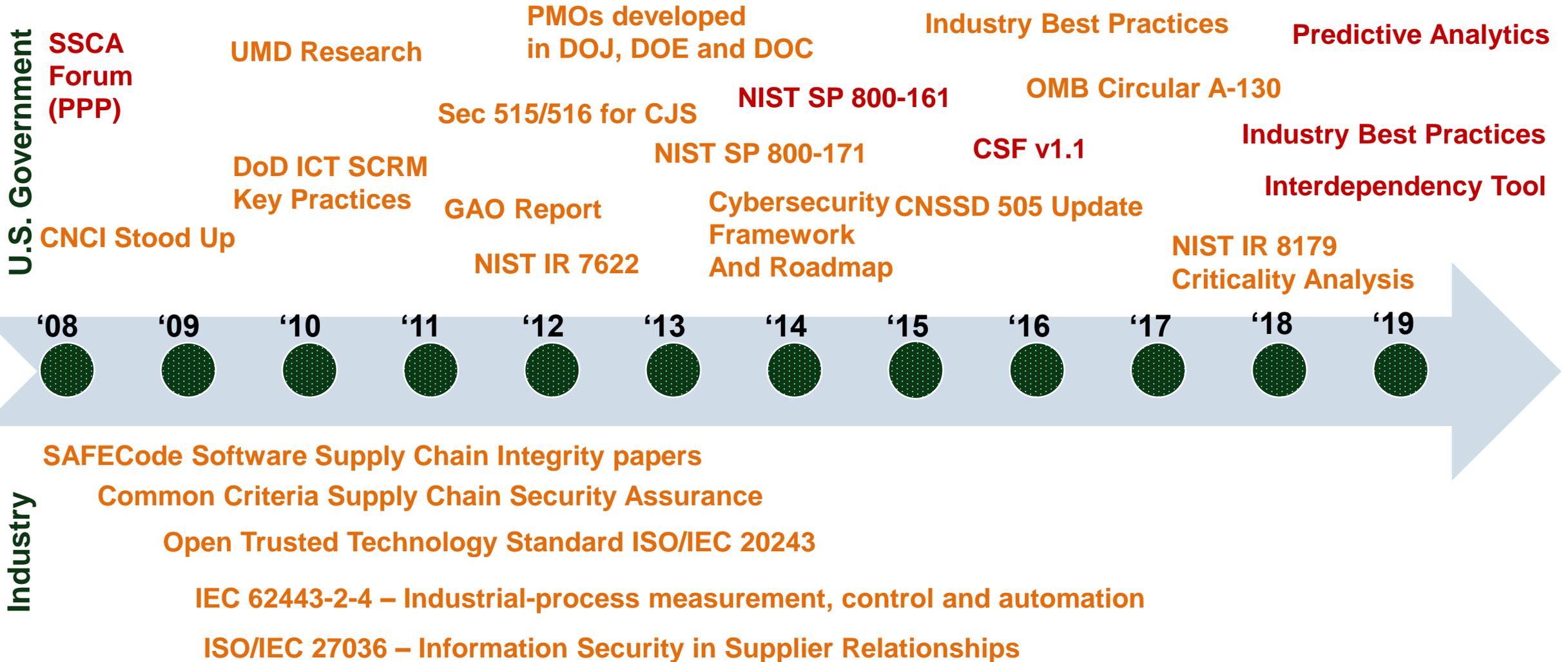
“Process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/OT product and service supply chains.”

- OMB A-130

> NIST's C-SCRM Program



Existing and Emerging Research, Policy, Standards, and Guidance



> Provenance

- **One of the more difficult-to-implement controls**
- Included first in NIST IR 7622 and then in NIST SP 800-161
- Subsequently in OMB A-130 and other policy documents
- **One of the most effective (anecdotally) C-SCRM tools**
- Can't manage what you don't know
- Automate the knowing
- **Current tools tend to be**
- Expensive
- Proprietary
- Unknown (by customers)

> Resources

C-SCRM Project

<https://csrc.nist.gov/scrm>

Software & Supply Chain Assurance Forum

<https://csrc.nist.gov/scrm/ssca>

Cybersecurity Framework v1.1

<https://www.nist.gov/cyberframework>

Celia Paulsen
cpaulsen@nist.gov

Jon Boyens
boyens@nist.gov



Supply Chain Assurance: Validating the Integrity of Servers and Client Devices



> Problem Statement

How do we know a delivered client/server matches
what we ordered...

... and only what we ordered?

Problems:

- Counterfeit products
- Substituted components
- Malware in system firmware/software
- Accountability/traceability in the supply chain

› Goals, Scope, and Status

- Tracking provenance increasingly recommended in USG and industry (NIST SP 800-161, CSF, ISO 27000 series, etc.)
- Tool set to help organizations verify the provenance and configuration of the systems (clients and servers) they purchase
- How? Work with industry to:
 - Identify useful artifacts
 - Determine how to generate artifacts as part of the manufacturing process
 - Understand how to measure and validate the artifacts before and during deployment in the operational network

> Scenarios

Scenario 1: Creation of Manufacturing Artifacts

An OEM or value added reseller creates verifiable artifacts that bind platform attributes to a root of trust in the PC/server.

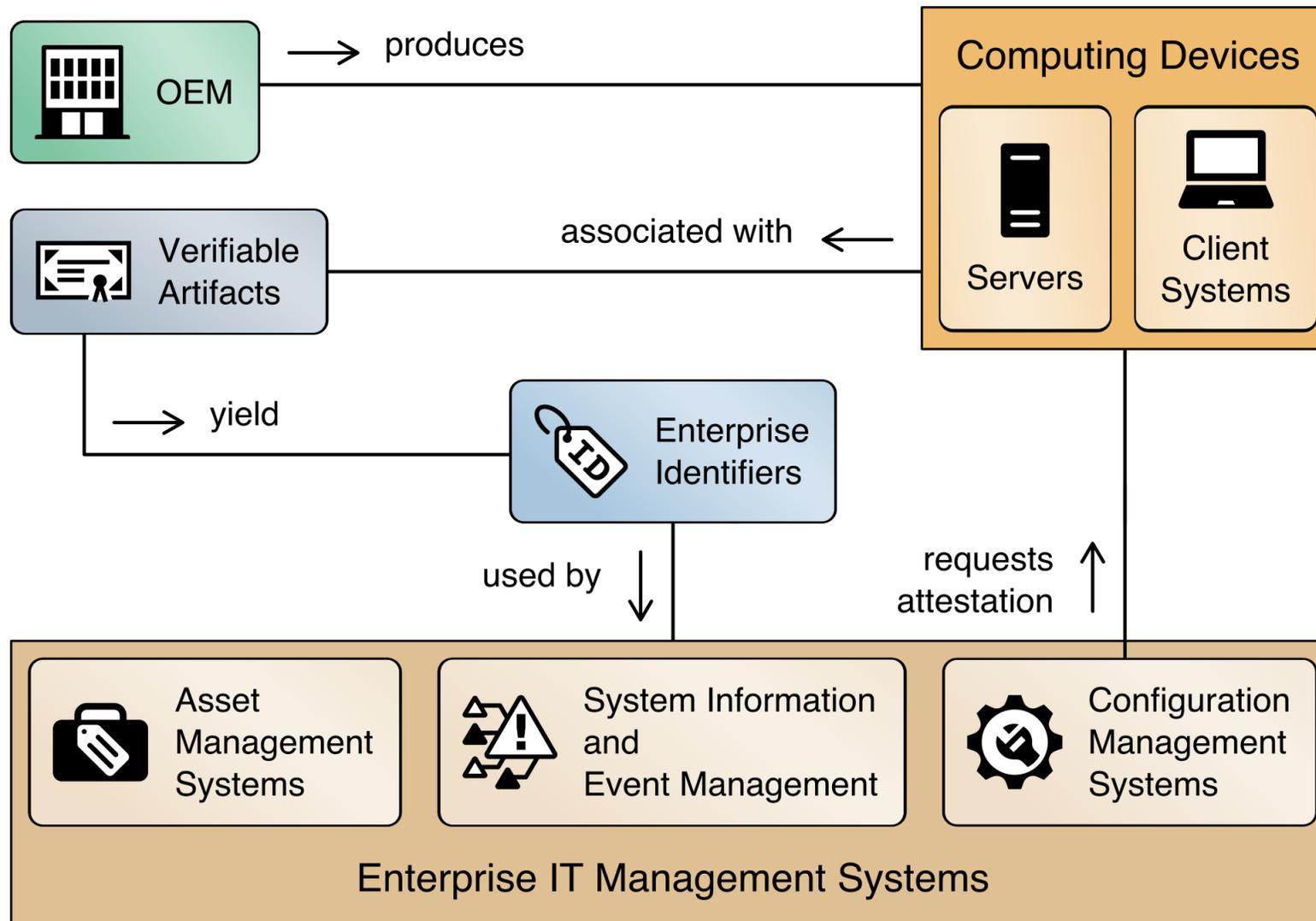
Scenario 2: Verification of Components During Acceptance Testing

IT Administrator receives a computing device through non-verifiable channels (e.g., off the shelf at a retailer) and wishes to confirm provenance, completeness, and establish authoritative asset inventory as part of an asset management program.

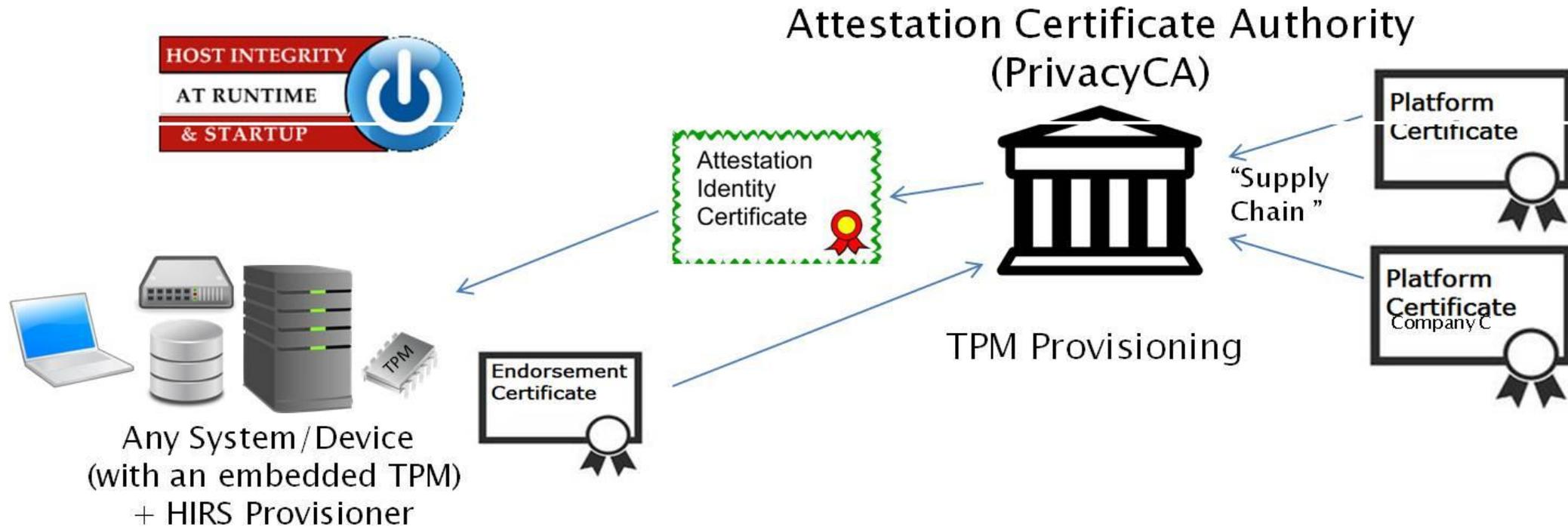
Scenario 3: Verification of Components During Use

IT administrator wishes to verify the platform attributes of deployed systems against the manufacturer's artifacts and inventory as provisioned in the asset and configuration management systems.

> Notional Architecture



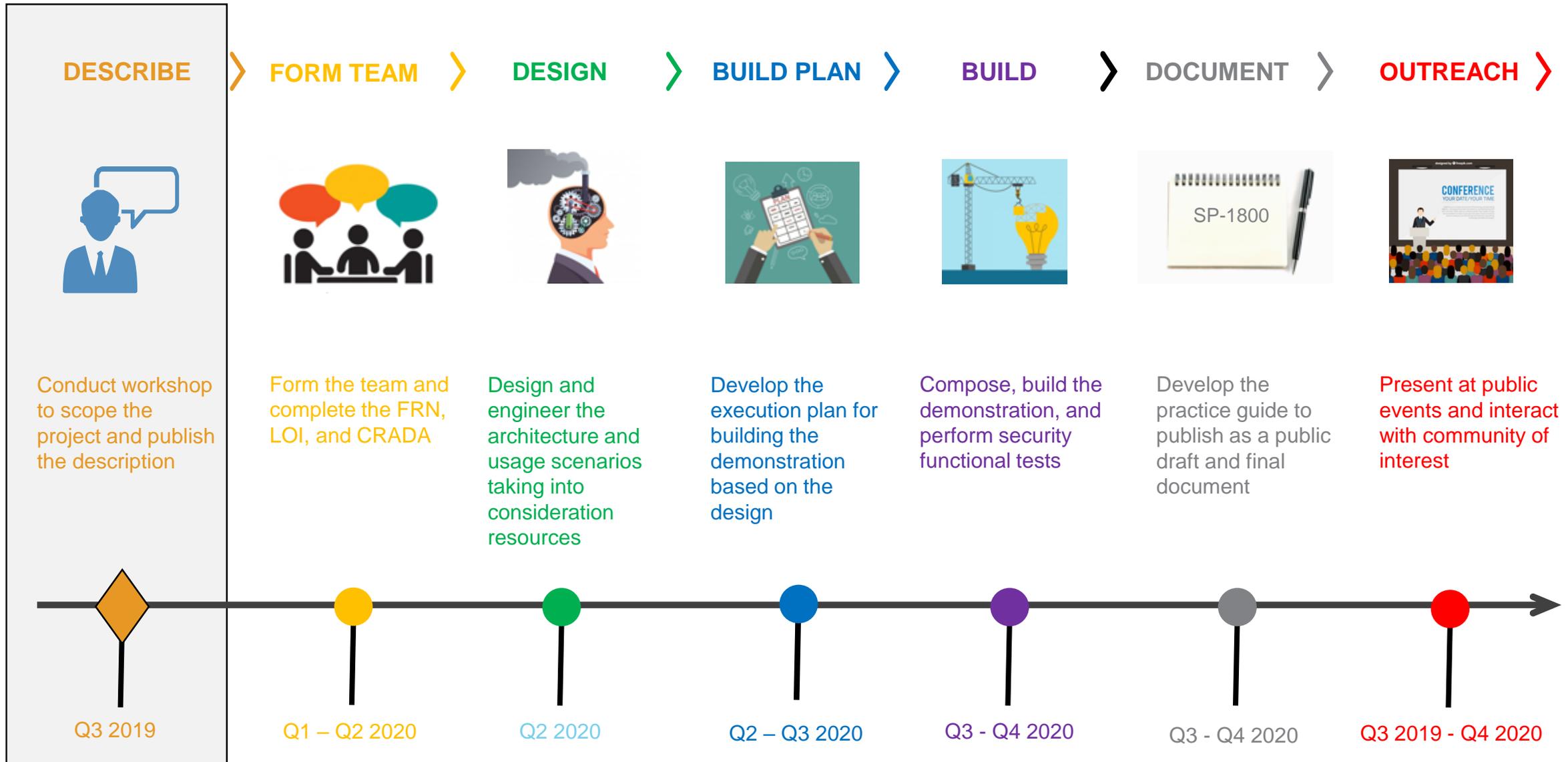
> Example: NSA HIRS Project



Reference: NSA Cyber Github

Open source tool and usage guides available at: <https://github.com/nsacyber/HIRS>

Proposed Project Execution Timeline



> Next Steps

Supply Chain Assurance: Validating the Integrity of Servers and Client Devices

Publish a Project Description and request for comment on NCCoE's website:

- **Submit comments via online or via email to supplychain-nccoe@nist.gov**
- **Public comment period of 30 days**

Stay tuned for a call for collaborators via a Federal Register Notice (FRN):

- **Look out for email from us announcing FRN**
- **Check status on project webpage:**

<https://www.nccoe.nist.gov/webform/cyber-supply-chain-risk-management-c-scrm-validating-integrity-servers-and-client-devices>

> NCCoE Supply Chain Project Team: Contacts / Roles

| | | |
|--------------------------|-------------------------------------|--|
| Nakia Grayson | NIST/NCCoE – Project Lead | nakia.grayson@nist.gov |
| Andy Regenscheid | NIST – Senior Engineer | andrew.regenscheid@nist.gov |
| Murugiah Souppaya | NIST/NCCoE – Senior Engineer | murugiah.souppaya@nist.gov |
| Tyler Diamond | NIST – Project Engineer | tyler.diamond@nist.gov |
| Tim Polk | NIST/NCCoE – Senior Engineer | william.polk@nist.gov |
| Celia Paulsen | NIST – Supply Chain Technical Lead | celia.paulsen@nist.gov |
| Jon Boyens | NIST – Supply Chain Project Lead | jon.boyens@nist.gov |
| Chris Brown | MITRE/NCCoE – Project Lead | cjbrown@mitre.org |
| Teresa Thomas | MITRE/NCCoE – Outreach & Engagement | tdthomas@mitre.org |



Trusted Computing Architecture





**Break
until 10:10am**





Industry Session



> Industry Panel Q&A



> Wrap Up: We Value Your Feedback

Do you:

- Have additional comments/feedback regarding our project?
- Have an idea that you think the NCCoE should pursue?
- Know of an event where NCCoE should present?

Please engage with us: supplychain-nccoe@nist.gov



<http://www.nccoe.nist.gov>



301-975-0200



nccoe@nist.gov