DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Providing Cybersecurity Inventory, Compliance Tracking, and C2 in a Heterogeneous Tool Environment

Joseph L. Wolfkiel

Secure Configuration Management Lead Engineer

May 2018

Disclaimer

The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.

Overview

- Objective and Problem Statement
- Defining Terms
- Building an Enterprise Inventory and Compliance Baseline
- Today's Homogeneous C2 and Reporting Environment
- Conducting Enterprise Cyber C2 in Today's Environment
- Heterogeneous Environment of the Future
- Comparative Challenges
- Stuff We Think We Can Do
- Stuff We Still Have to Figure Out

Objective and Problem Statement

- **Objective: To help attendees understand the challenges in conducting Cyber Command and Control (C2) and reporting in the evolving DoD and commercial cyberspace environment**
- **Problem Statement:**
  - **The DoD has been moving to a common cybersecurity toolset for 10+ years**
    - **Starting with Host-Based Security System (HBSS) in 2004-2005**
      - **HBSS included management agent & Host Intrusion Prevention System (HIPS)**
      - **Moved to single AV product integrated with HBSS**
      - **Added enterprise**
        - Compliance checking
        - "Device Control Module"
        - Application whitelisting
        - Software inventory
    - **Common vulnerability and STIG scanner acquired as Assured Compliance Assessment Solution (ACAS)**
  - **Current plans go to per-component best of breed products**
  - **US Cyber Command and the Joint Forces Headquarters, DoD Information Network (JFHQ DoDIN) need to provide enterprise defense**

Defining Terms

- Cybersecurity: Prevention of damage to, protection of, and restoration computers and networks, to ensure availability, integrity, authentication, confidentiality, and nonrepudiation (DoDI8500.01, 14 Mar 14)
- Inventory: A complete list of items such as property, goods in stock...(bing.com)
- Compliance: The state or fact of according with or meeting standards (bing.com)
- Command and Control (C2): Exercise of authority and direction of assigned forces (U.S. Army FM 3-0)
- Heterogeneous: composed of parts of different kinds… (Dictionary.com)

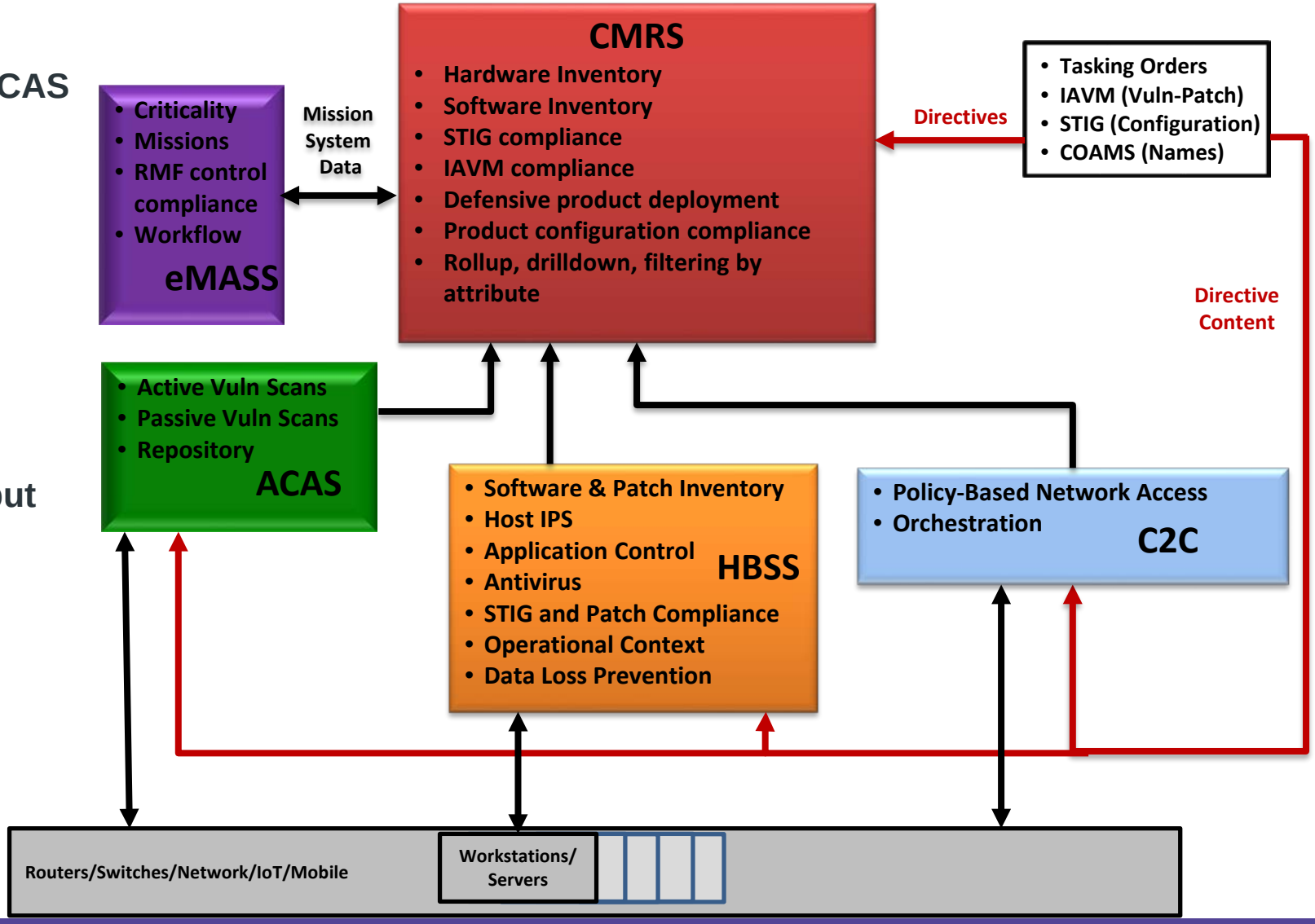
Building an Enterprise Inventory and Compliance Baseline

Cumulative process, following NIST 8011 and CIS basic security control concepts

- Hardware Asset Management (HWAM) - Asset ID and inventory, operational context
- Software Asset Management (SWAM) - Software inventory & install/execution control
- Vulnerability Management (VUL) - Vulnerability awareness and patch priority
- Security Configuration Management (CONF) - Security Technical Implementation Guidance (STIG) & Individual Configuration Directives
- Anti-Malware - Host Intrusion Prevention System and Antivirus
- Insider Threat Mitigations - Data Loss Prevention (DLP), user behavior analytics, and knowledge management (KM)

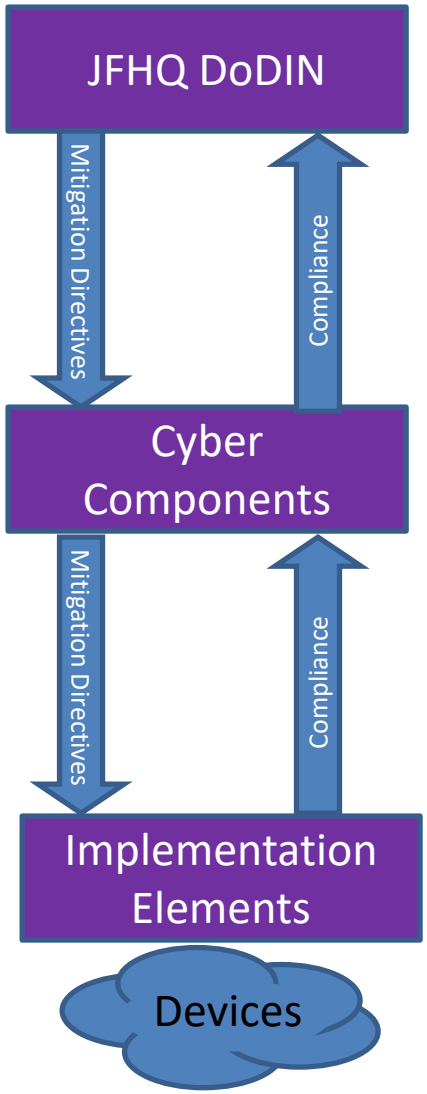
Today's Homogeneous C2 and Reporting Environment - Multiple Tools, But Only One Per Capability

- HBSS and ACAS are Primary Sensors
- Plans to add C2C Sensor
- All data reported to CMRS or input to eMASS



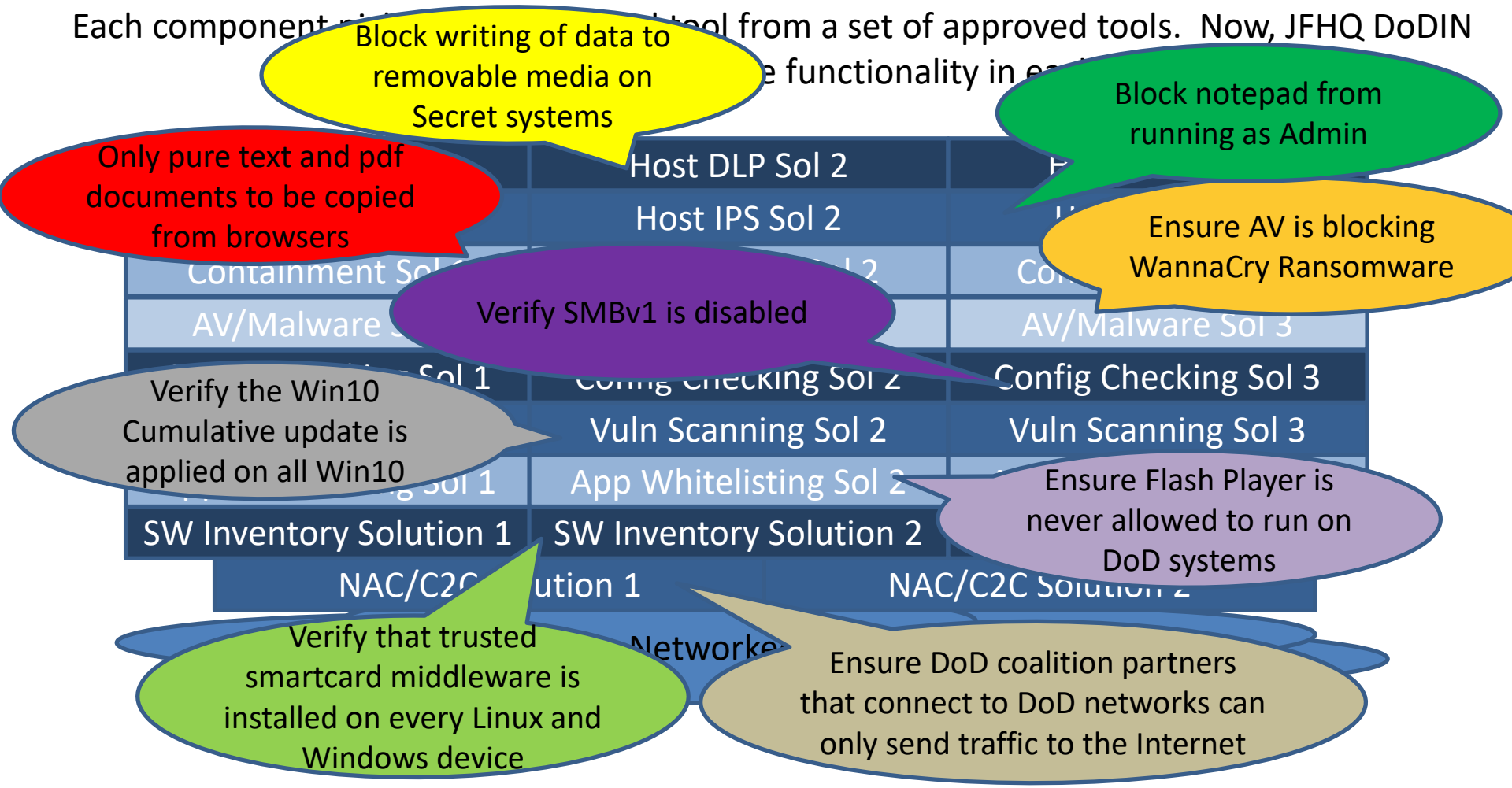
Conducting Enterprise Cyber C2 in Today's Environment

- **Which Devices are Permitted on the Network**
  - **Unsupported products**
  - **TBD Enterprise C2C policy**
- **Application of Patches**
  - **The IAVM process**
- **Scanning and Reporting of Vulnerabilities**
  - **ACAS Tasking Orders and the IAVM process**
- **Directing Secure Configurations**
  - **STIG process**
- **Directing Malware Mitigations**
  - **Custom Host Intrusion Prevention System Signatures**
  - **Minimum AV signature ages and scan frequency**



Heterogeneous Environment of the Future:
Best of Breed Tools for All of Today's Capabilities Then Some

Each component ... tool from a set of approved tools. Now, JFHQ DoDIN ... functionality in ...



Comparative Challenges

Homogeneous

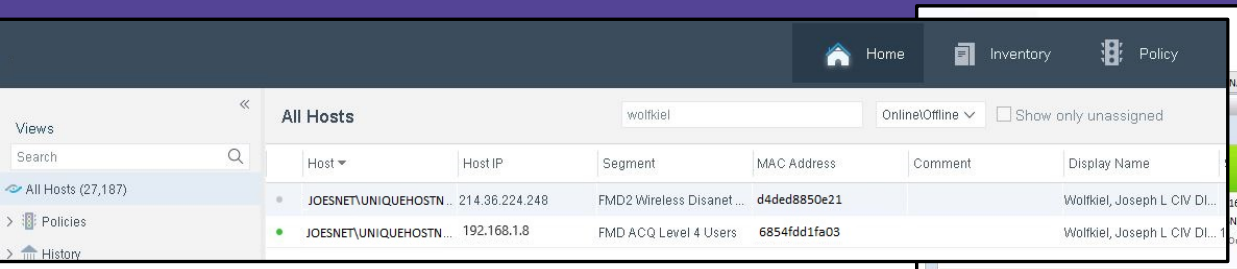
- Implement enterprise protective or defensive measures
- Automatically collect directive compliance data
  - Broken out by device count, location, organization, and/or accreditation boundary
- Event analysis to determine how frequently measures are being invoked

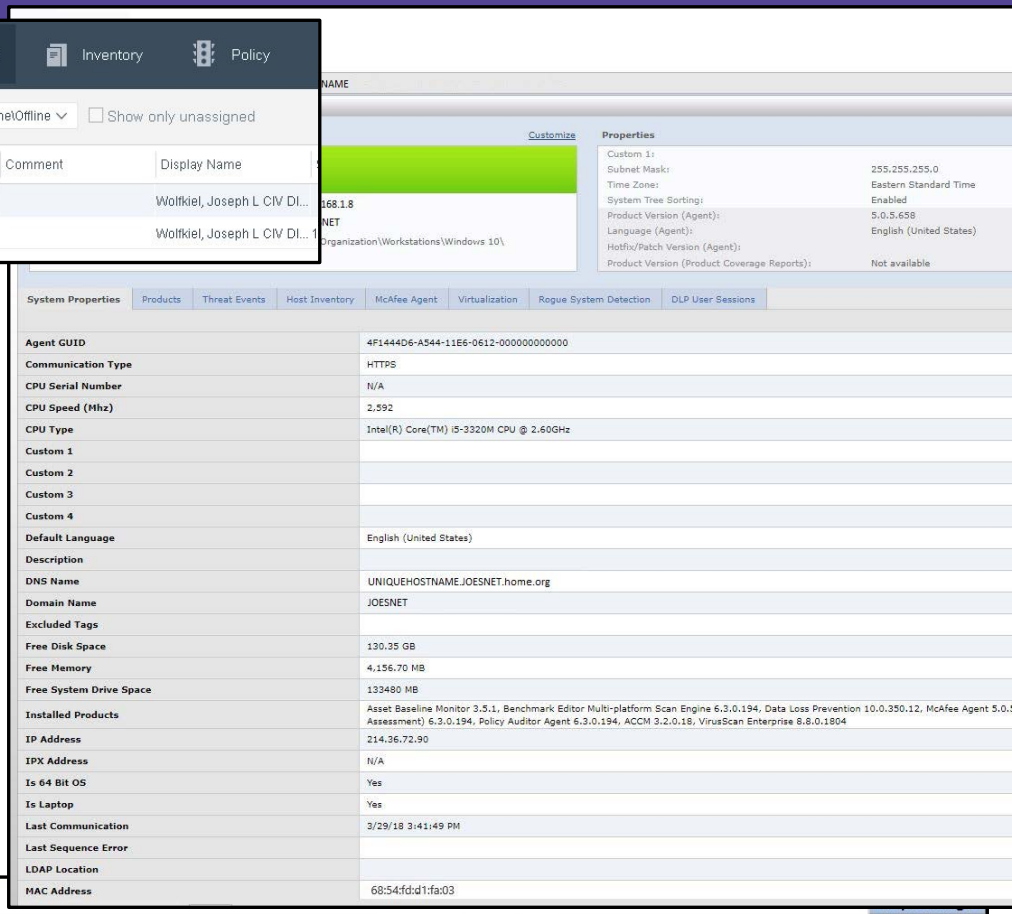
Heterogeneous

- Implement enterprise protective or defensive measures in a *tool-agnostic way*
- Automatically collect compliance data
  - Broken out by device count, location, organization, and/or accreditation boundary *and correlate the compliance indicators between different tools*
- Analyze event data to determine how frequently measures are being invoked *when different events are being produced per tool for the same incident*

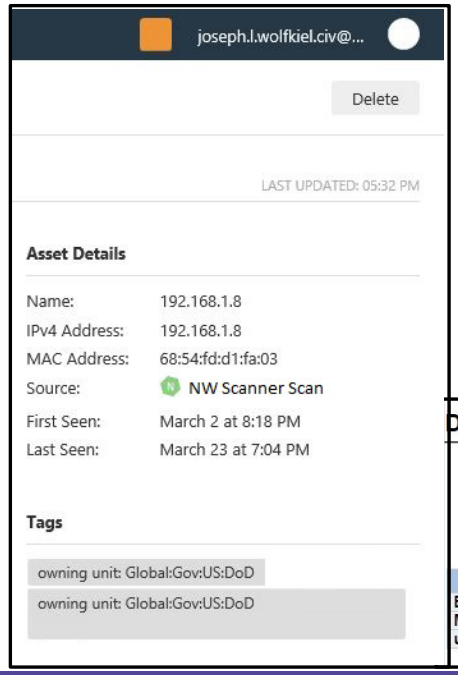
Future: Factor in all protective and defensive capabilities to determine, per attack vector, if a device population is protected from a threat or class of threats

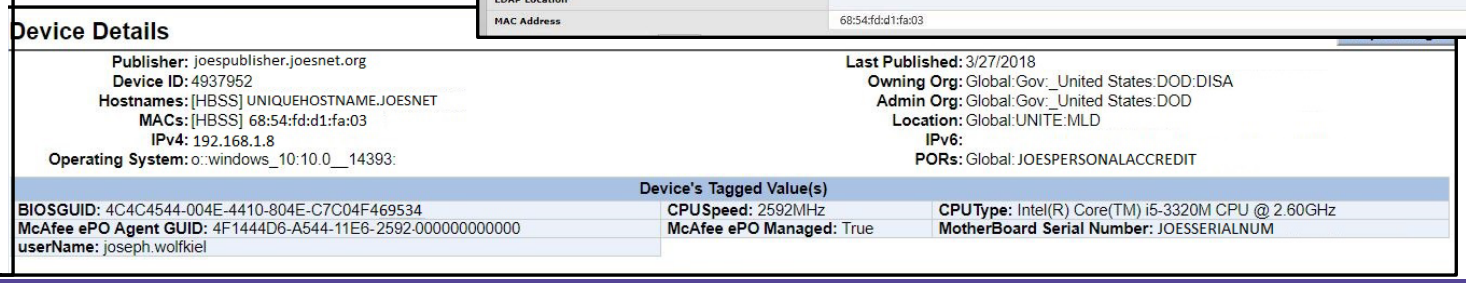
Stuff We Think We Can Do – Asset Identification/Correlation





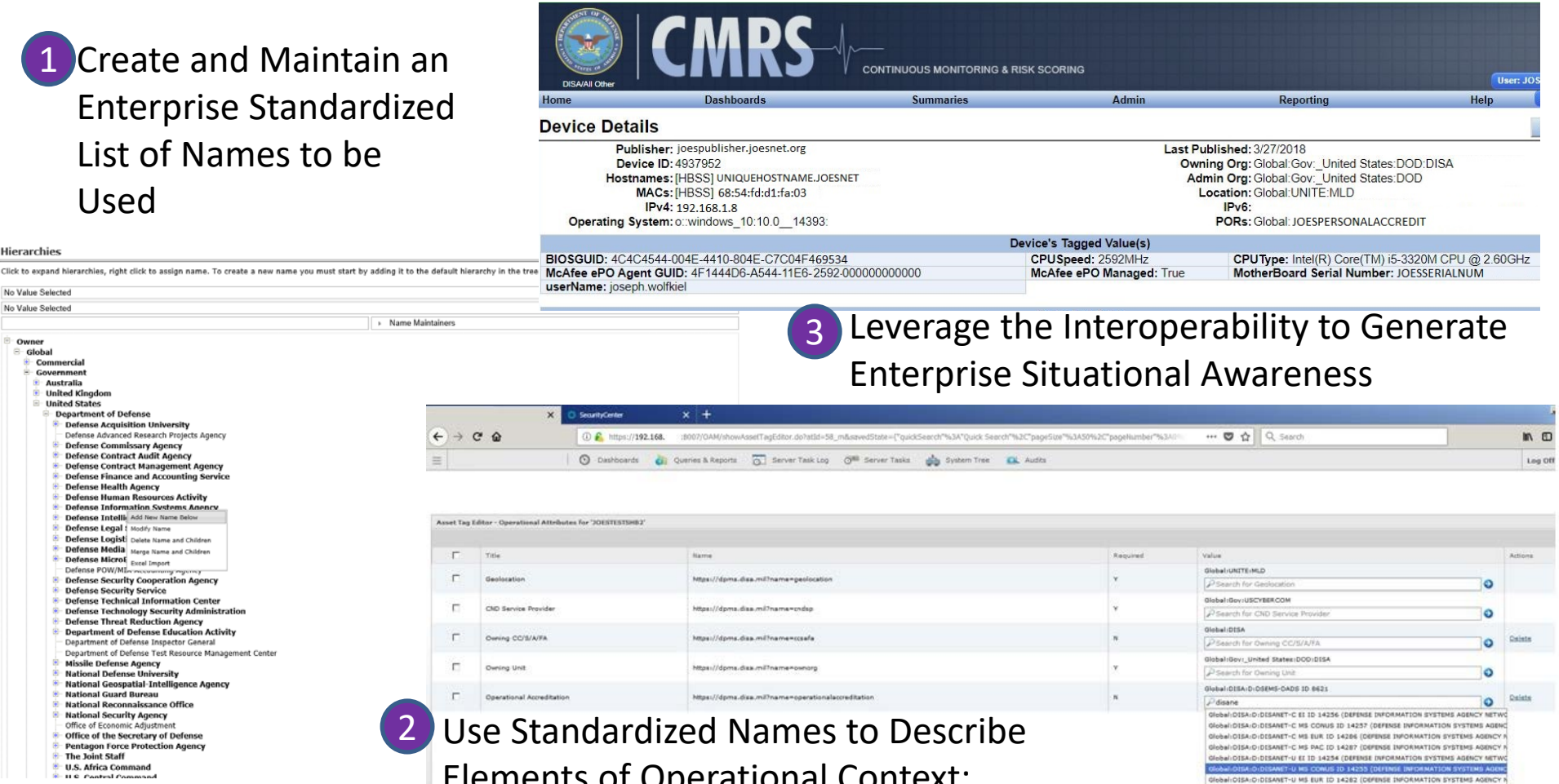
Same Device? How do you tell? IP, MAC, Hostname, Serial Number, BIOS GUID, Software GUID?





Stuff We Think We Can Do – Asset Operational Context/Characterization

1. Create and Maintain an Enterprise Standardized List of Names to be Used



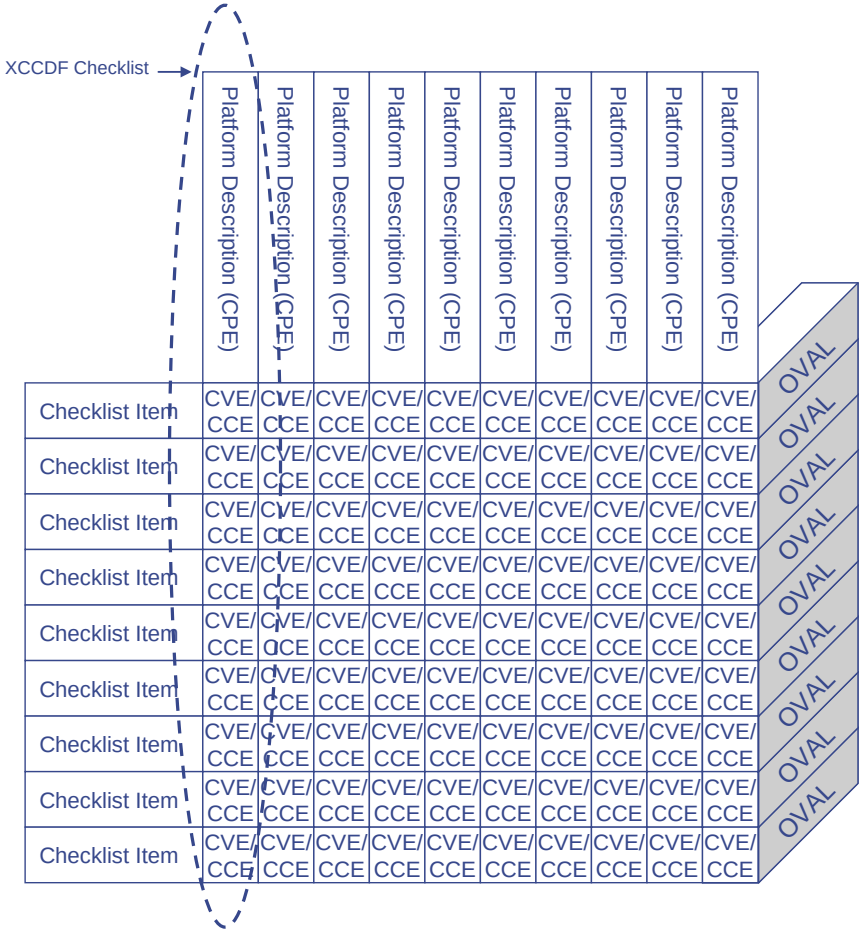
3. Leverage the Interoperability to Generate Enterprise Situational Awareness

2. Use Standardized Names to Describe Elements of Operational Context:
Who owns it? Where is it? What accreditation boundary does it belong to?

Stuff We Think We Can Do – Patch and Vulnerability Management, Config Compliance

- **How? Leverage the NIST Security Content Automation Protocol**

- OVAL – Language to check for settings and software in a given Operating System
- XCCDF – Checklist automation (STIG)
- CVE – Standardized IDs for vulnerabilities
- CCE – Standardized IDs for settings
- CPE – Standardized names for hardware and software



Stuff We Still Have to Figure Out

- **Standard policies and compliance reporting for:**
  - **Antivirus**
  - **Data loss prevention**
  - **Host IPS**
  - **Application whitelisting**
  - **Containment**
  - **Other TBD**

- **Way Ahead: Try to leverage SCAP concepts**
  - **Minimum compliance set per required function**
  - **Compliance measures in “benchmarks” per tool and/or capability set**
  - **Resolve compliance assessments to pass/fail**

Questions?

rate us

take the 3-question survey
available on the AFCEA 365 app

visit us

DISA Booth # 443

follow us

Facebook/USDISA

Twitter/USDISA

www.disa.mil

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**