CMMC Update:
Mastering the Basics Part 2

Current As Of: November 2023

TODAY'S SPEAKERS

Amira Armond

President

Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum

Vince Scott

CEO

Defense Cybersecurity Group
INFRAGARD National SME Cyberwarfare

Scott Whitehouse

Director of Compliance Services

C3Integrated Solutions

Sponsored by:

COALFIRE FEDERAL

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- Contractual obligation to comply with National Institute of Standards and Technology (NIST) 800-171Rev2
  - Companies not complying sufficiently under current regulation
  - Does not negate obligation to meet the contractual requirements
- CMMC announced Jul ’19 -- 3rd Party Assessments to ensure 800-171 implementation in the future
  - CMMC 2.0 announced Nov ’21
- **DRAFT NIST 800-171Rev3 released 10 May 23**
  - Final draft out for comment – Closes January 12th
  - NDIA Corporate members can work with the Cybersecurity Division
- **CMMC rule with OMB**

Sponsored by:

Timeline Summary

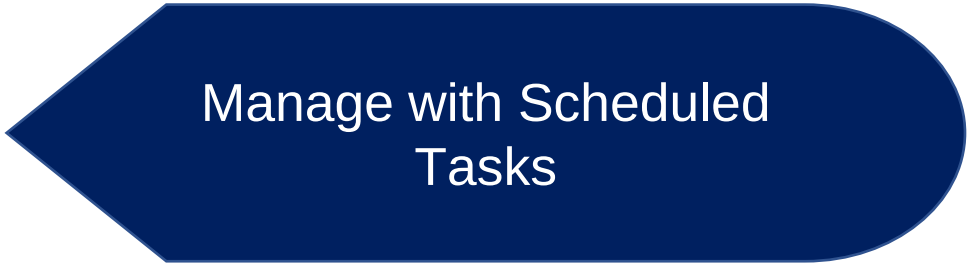
- **2 Processes moving the goal posts running simultaneously**
- **NIST 800-171 Rev3 Final – Comments 12 Jan**
  - Jan – Feb 24 with Guidebook for Assessments
- **CMMC: Interim Final Rule (IFR) vs Notice of Proposed Rulemaking (NoPRM)**
  - IFR: As early as Jan 24 3rd party assessment requirements may appear in contracts
  - NoPRM: Likely Q1 CY25 before assessment requirements hit

Big Realization

- Two types of security controls:

- Security controls that don't fail over time

- Security controls that fail on their own over time



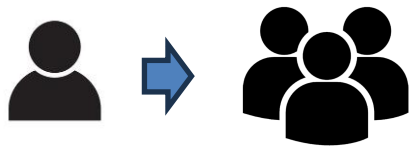
Why Change Management

3.1.8 Limit logon attempts
3.1.9 Security notices
3.1.10 Session lock
3.1.11 Terminate user session
3.1.13 Encrypt remote sessions
3.1.14 Route remote access
3.1.17 Encrypt wireless access
3.1.19 Encrypt mobile device CUI
3.3.1 Create and retain audit logs
3.3.2 Audit logs identify user
3.3.3 Audit record reduction and reporting
3.3.4 Alert if audit logs fail
3.3.7 Network time
3.3.8 Protect audit information
3.3.9 Limit management of audit info
3.4.2 Security configuration settings
3.4.6 System least functionality
3.4.7 Restrict non-essential functions
3.4.8 Blacklisting and whitelisting software
3.4.9 Control user-installed software
3.5.1 Identify
3.5.2 Authenticate
3.5.3 MFA

3.5.4 Replay-resistant authentication
3.5.7 Password complexity
3.5.8 Prohibit password reuse
3.5.10 Protect passwords
3.5.11 Obscure passwords
3.10.1 Control physical access
3.10.2 Protect support infrastructure
3.13.1 Monitor and control boundaries
3.13.3 Separate system functionality
3.14.4 Shared system info transfer
3.13.5 Subnetworks
3.13.6 Deny traffic by default
3.13.7 Split tunneling
3.13.8 Protect CUI in transit
3.13.9 Terminate network connections
3.13.11 FIPS validated cryptography
3.13.12 Collaborative computing devices
3.13.13 Control mobile code
3.13.15 Protect communication authenticity
3.13.16 Protect CUI in storage
3.14.2 Anti-malware
3.14.4 Anti-malware definitions
3.14.5 Anti-malware scans

Requirements that are implemented (and tend to stay implemented) if we design / build systems correctly

Types of Changes

Types	Description	Approvals
Minor	Doesn't change security, low risk, low impact	
Major	Could harm security or systems, complex, costly	
Emergency	Major change that needs to be expedited	
Routine	Follows a well-established procedure, considered pre-approved	

Security Impact Analysis

Change Management Policy

4.6. Security Impact Analysis

a) When significant changes are planned for, or made to, a system, the change sponsor shall conduct a security impact analysis as part of planning. The **<CIO>** or **<CISO>** will review this analysis before approving or disapproving the change.

b) The following security risk impact analysis activities may be incorporated into the change control process (as applicable):

   1) Review NIST-published vulnerability databases and recommended security checklists to understand whether the change will introduce new security risks.
   2) Identify whether the changed system will meet configuration management guidelines for secure configurations.
   3) Identify sensitive information in the changed systems and the risks to confidentiality during or after the change.
   4) Identify the security mechanisms for integrity and availability. For example, planning for backups or failover.
   5) Identification of how the changed system will be securely managed. For example, configuring administrative access via HTTPS

Change Tracking, Logging, Approval

CHANGE_DB

ID	Short Change Title
101	Update M365 and Endpoint Manager configs to reflect lessons learned
102	Microsoft Teams vs Teams Machine-Wide Installer
103	Conditional access policy for privileged accounts, expire token sooner
104	Update sentinel configurations for Reference Architecture

Activity Log

V. Amira Armond (2/21/2021 10:56 AM):
Deployed

V. Amira Armond (2/18/2021 8:38 AM):
Ready for deployment if approved.

V. Amira Armond (2/18/2021 8:34 AM):
Scheduled reboot script took. Test computer installed winc
updates and rebooted overnight. No hibernate or sleep oc

V. Amira Armond (2/17/2021 4:24 PM):
Tested Windows 10 update ring settings - successful.

Planning: What is the cost of this change?

0

Planning: How many labor hours will this take?

4

Planning: Perform a security impact analysis. Document results below.

Improves security by forcing reboots and software patches to occur on workstations. This change does not adversely affect any security requirement.

April 2022

[redacted] commented
Reviewed on CAB on 2022-04-04. Change successfully completed - SVT

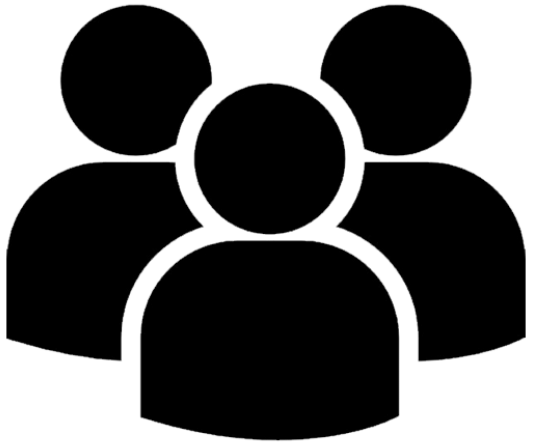
March 2022

[redacted] commented
Change will increase security posture of Azure Presence in cloud. Approved on CAB on Mar 15, 2022 - SVT

Sponsored by:

Change Approval Board (CAB)

- Expected for major and emergency changes
- Group (at least 2 people) with voting
- Meeting notes a primary source of evidence
- Formal approval and review of changes



Incident Response

- **What is an *Incident?***
  - NIST – “An occurrence that actually or imminently **jeopardizes**, without lawful authority, the **confidentiality**, **integrity**, or **availability** of information or an information system; **or** constitutes a violation or imminent threat of **violation of law, security policies, security procedures, or acceptable use policies**”
  - 7012 – ““Cyber incident” means actions taken through the use of computer networks that **result** in a **compromise** or an actual or potentially **adverse effect** on an **information system and/or the information residing therein**.”
  - **What is your definition?**

Incident Response

- **What is a *reportable incident?***
  - Reportable when an incident meets criteria defined by an applicable regulation
    - DFARS 7012 – When the Contractor discovers a **cyber incident** that affects a **covered contractor information** system **or** the **covered defense information residing therein**, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall - **Rapidly report** cyber incidents to DoD at https://dibnet.dod.mil.
- **Everyone will experience cyber incidents regularly**
  - Governments definitions are broad
  - If you have gone a year without an incident likely not looking hard enough
  - **Differentiate between incidents and reportable incidents**

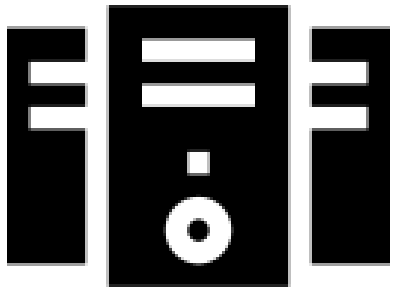
Incident Response

- **How do I improve my ability to respond to an incident?**
  - Conduct annual Incident Response exercises
  - Insist upon ***working knowledge*** of
    - Regulations your company must follow (contractually…know your contracts)
    - What makes an incident reportable
    - Processes for reporting
- **Best practice: ensure your business operations personal participate in the exercises**
- **Make your exercises hard to optimize your preparation**

Incident Response

- **Consequences of fumbling reporting requirements are potentially high**
  - EX: SEC and Solar Winds
- **Stay up-to-date on threats and your organization's information security reporting requirements**
  - **Include reporting requirements in your incident response plan**
    1) A complete list of reportable incident types for each applicable regulation
    2) Corresponding timeframes
    3) Report format
    4) To whom the report must be submitted
- **Example: DFARS 7012 governs CUI processing/handling/storing and includes its own Incident Reporting requirements**
- ***Your Incident Response Plan is a living document***

Configuration Management – Hardware Planning



Asset identification and categorization

- **Hardware**
  - **Laptops**
  - **Multi-function copiers**
  - **Servers**
  - **Cloud systems**
  - **IoT devices**
  - **Removable storage / flash drives**

Applies to pre-production and production assets

Configuration Management – OS Planning

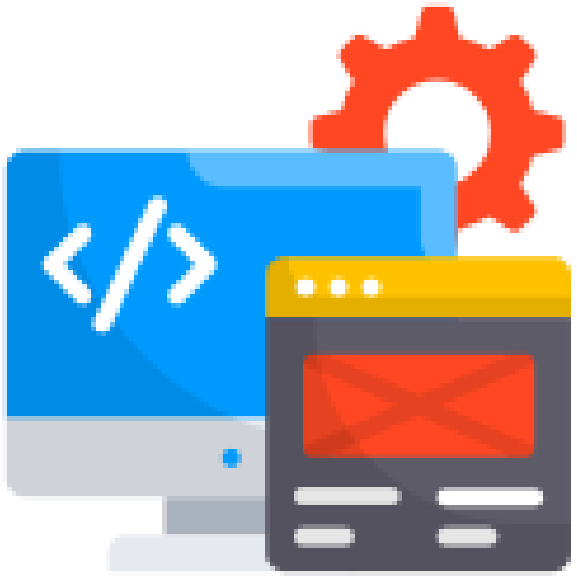
Asset identification and categorization

Operating System
- Windows 10/11
- MacOS
- Linux
- ESXi

Applies to preproduction and production assets

Sponsored by:
COALFIRE FEDERAL

Configuration Management – Software Planning



Asset identification and categorization

- **Software**
  - **Identify full list of approved applications**
  - **Support tools**
  - **Endpoint installed software**
  - **Mobile apps**
  - **Administration utilities**

Applies to pre production and production assets

Configuration - Planning

Define a frequency of review

Create a process for establishing and implementing configurations (hint…. Change management is part of this)

Ensure your process adheres to standards for secure system design. See NIST SP 800-160.

Configuration Management – Getting Started

List

List all intended configurations

- Document ports, protocols, services, functions which are REQUIRED for patterns of business activity

Map

Map configurations to compliance requirements

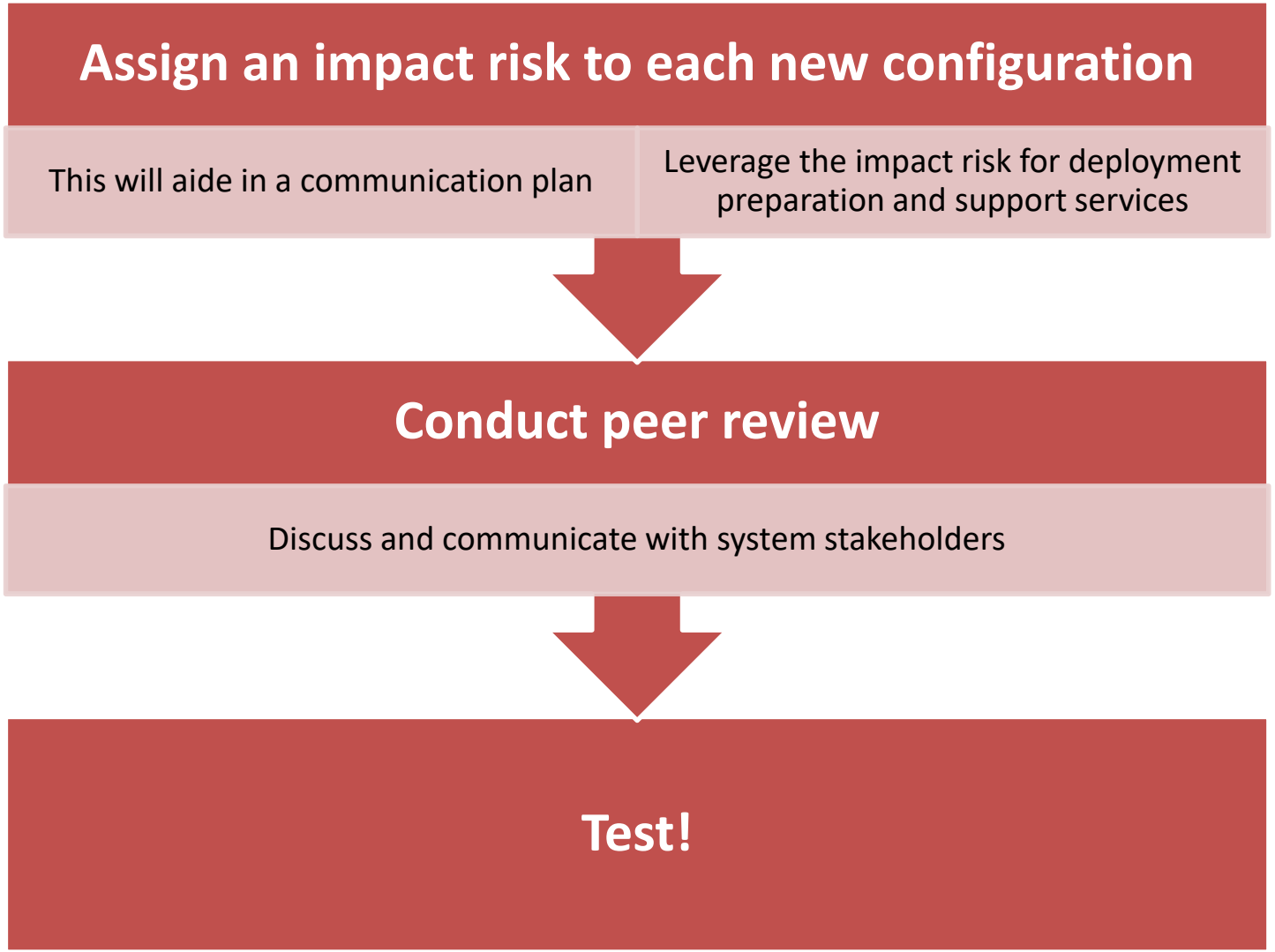
- Note many may be security best practices others will be compliance requirements

Review

Review available resources for guidance

- DoD STIGS
- OWASP vulnerability list
- Microsoft Security Baselines and Blueprints

Configuration Management – Document and Test



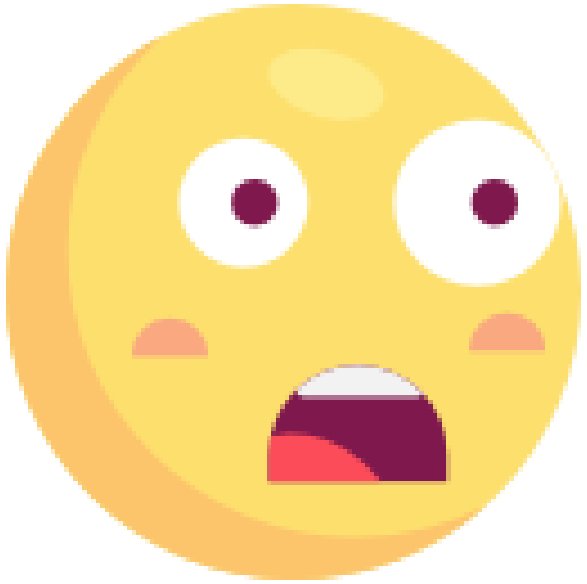
Configuration Management – Keep Testing

Vital step – failure to capture impact prior to deployment will impact future releases.

Capture challenges, remediate where possible.

Refer to previous mapping of configuration to compliance when challenges arise.

Configuration Management - Deploy



Deployment may be staged or big bang depending on the risk and environment size.

Assigning configurations does not mean they work!

Remember the verbs “Monitor” and “Implement”.

Configuration Management - Enhance

Monitor	Monitor security feeds for new risks
Monitor	Monitor for trends in vulnerabilities
Review and update	Review and update configurations based on the prescribed interval (semi-annual?)
Document	Document the review process (who, what, when, why)

Guest Question

- **Based on current draft, will CMMC be required for OTA contracts and CRADA or research contracts?**

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- Contractual obligation to comply with National Institute of Standards and Technology (NIST) 800-171Rev2
  - Companies not complying sufficiently under current regulation
  - Does not negate obligation to meet the contractual requirements
- CMMC announced Jul ’19 -- 3rd Party Assessments to ensure 800-171 implementation in the future
  - CMMC 2.0 announced Nov ’21
- **Final DRAFT NIST 800-171Rev3 – comments due 12 Jan 24**
- **CMMC rule with OMB**
- **Communicate with your MSPs/MSSPs/ESPs**
  - Be ready for implementation of the final rule

Sponsored by: COALFIRE FEDERAL

Rachel

Questions?

Sponsored by: