Cybersecurity

J. Brad Fuller
Director of Cyber Solutions
MartinFederal

MartinFederal

| Our Mission |

Our Mission is to be a company that supports and sustains a safe return of our nation's warfighter, astronaut, and deployed civilian through our daily efforts and driven success to exceed customer expectations.

| Our Vision |

Our Vision is for our employees to lead with ethics and to focus on developing innovative and efficient processes that will directly benefit our customers and their overall goals – from national security to geospatial research and development.

| Our Values |

Responsive.

Reliable.

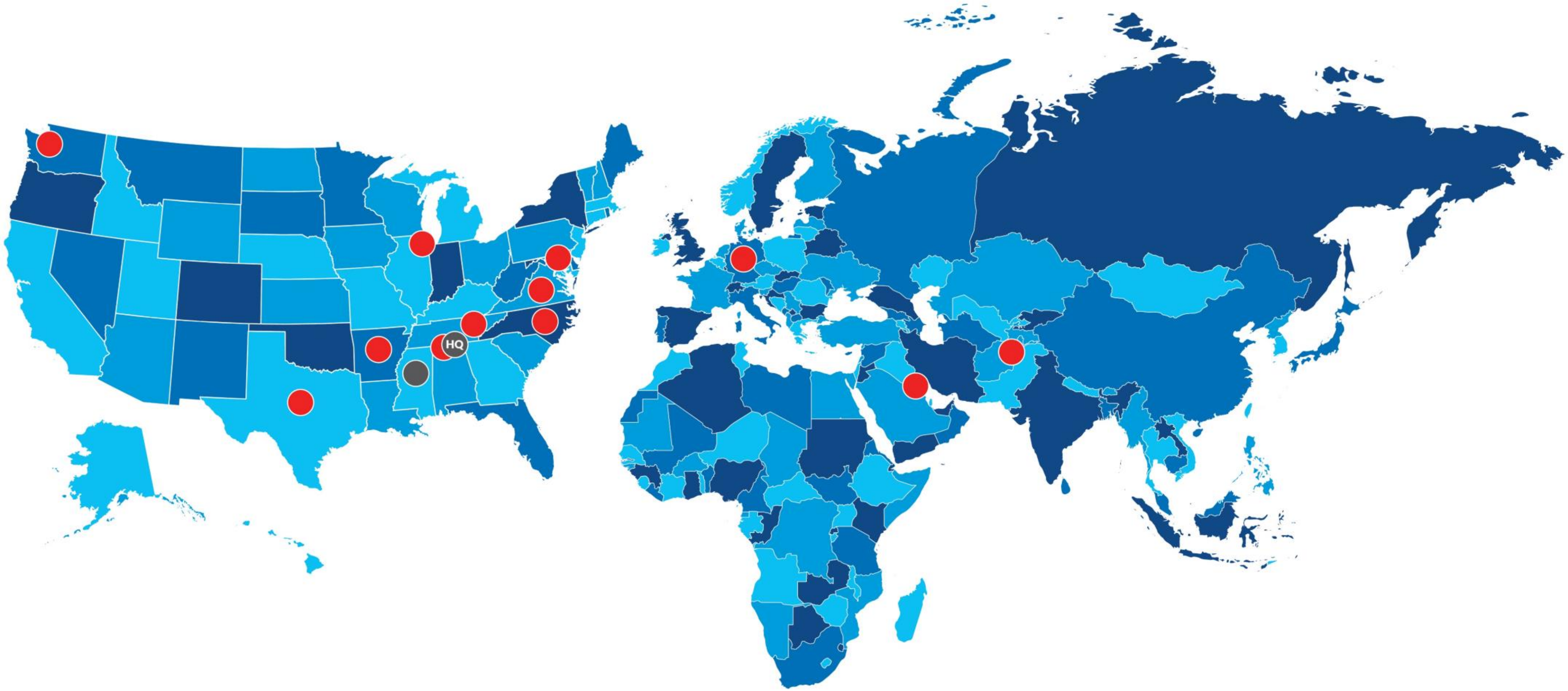
Resilient.

513 Madison Street SE
Huntsville, AL 35801
www.martinfed.com

100 Research Blvd.
Suite 215 Starkville,
MS 39759

MartinFederal

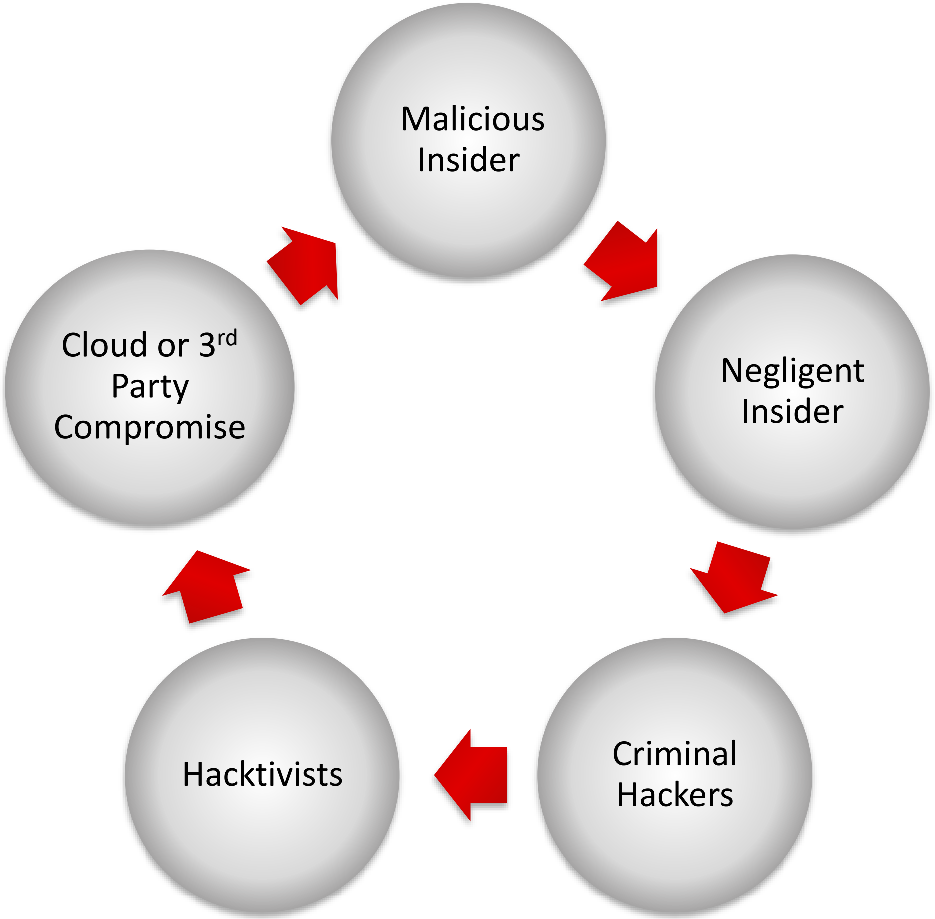
| Our Locations |



What Does a Data Breach Look Like?

The Threat Environment

- Growing incentive for insiders to abuse access to sensitive data for financial gain
- Disgruntled current and former employees exploit back-doors
- Theft of Intellectual Property Security compromise
  - Loss of sensitive client data
- Infrastructure downtime may lead to Dependent Business Interruption claim
- Intent is to disrupt and/or embarrass a target



- Unwary insiders susceptible to attacks that exploit traditional security controls (e.g. spear phishing)
- Users who fail to embrace “culture of security” will find ways to circumvent ‘inconvenient’ security controls
- Patience is a virtue. Tactics have evolved from “hit and run” to “infiltrate and stay”
- Industrialization - Black market exist for all types of personal information
- Proliferation of mobile platforms and BYOD policies creates new vectors

Vulnerabilities Around Employee Behaviors of Using Technology

82%

Of employees have read and understand their company’s policies regarding data privacy and information security

41%

Use their work computer or cellular device to access **confidential** company information

22%

Use **personal computing devices** that have not been approved by their company’s information technology (IT) department to do work at home

32%

Log into their work computer or cellular device using an **unsecured public network** (Wi-Fi)

31%

Use their work computer in **public settings** (e.g., while commuting, on airplanes/trains, at cafes)

34%

Share personal information (e.g., birthdate, employer name, job title) in profiles on social media sites

Personal Tasks and Security Measures

If you didn’t ask for it, don’t open it

If you download an application, keep it updated

Keep your anti-virus updated and running

Each account should have its own password

Double-check suspicious requests

Use your head

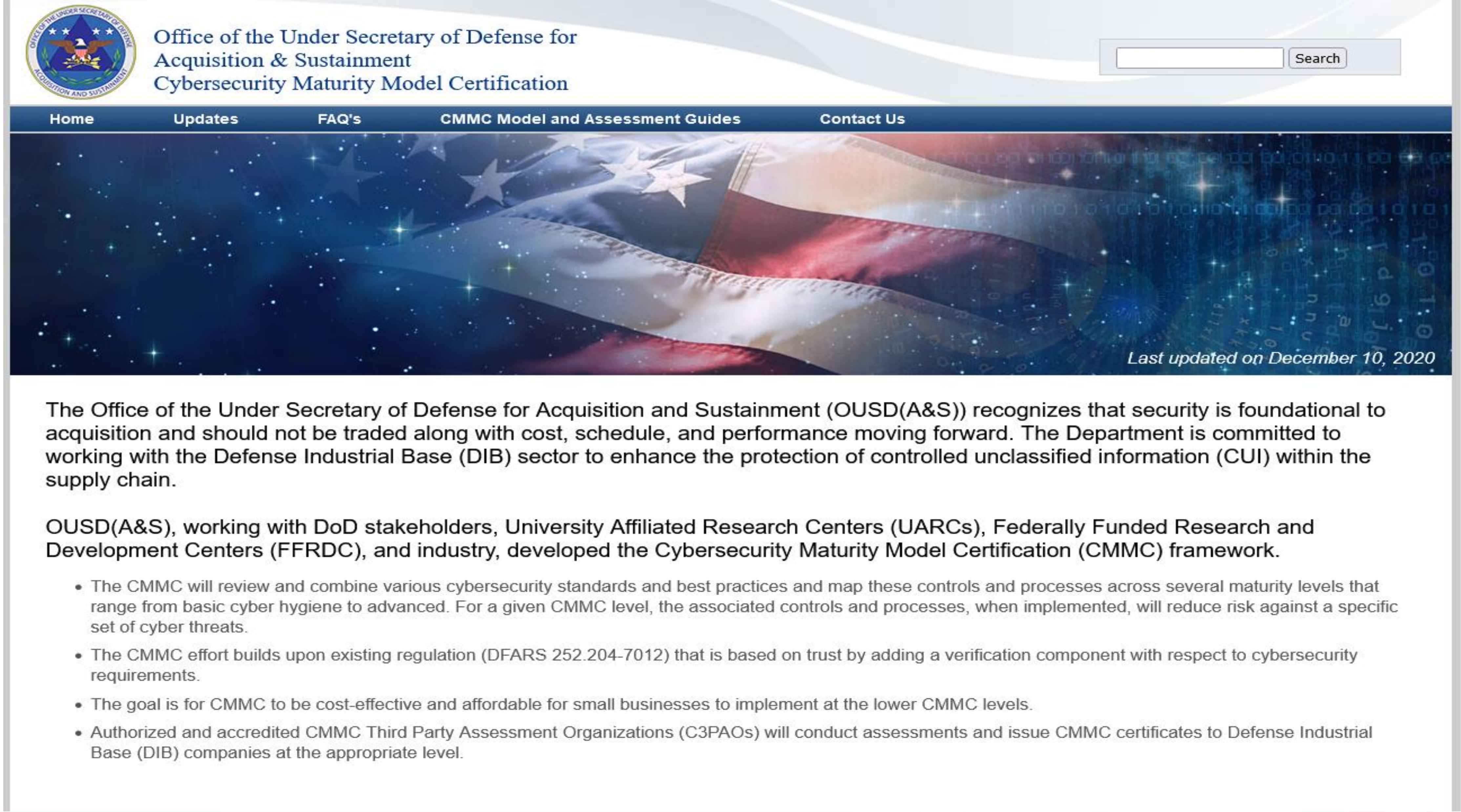
Report it

Cyber Defense & Response

- SIEM (Security Information and Event Management)
- SOC/CSOC (Security Operations Center)
- Endpoint Protection/Anti-Virus
- Threat Hunt
- Incident Response
- Digital Forensics
- Insurance and Reporting

Cybersecurity Industry Overview

- 80% of the Cybersecurity industry is simply marketing material
- Everyone needs to understand the questions to ask around Penetration Testing and Vulnerability Scanning
- THERE IS NO SILVER BULLET



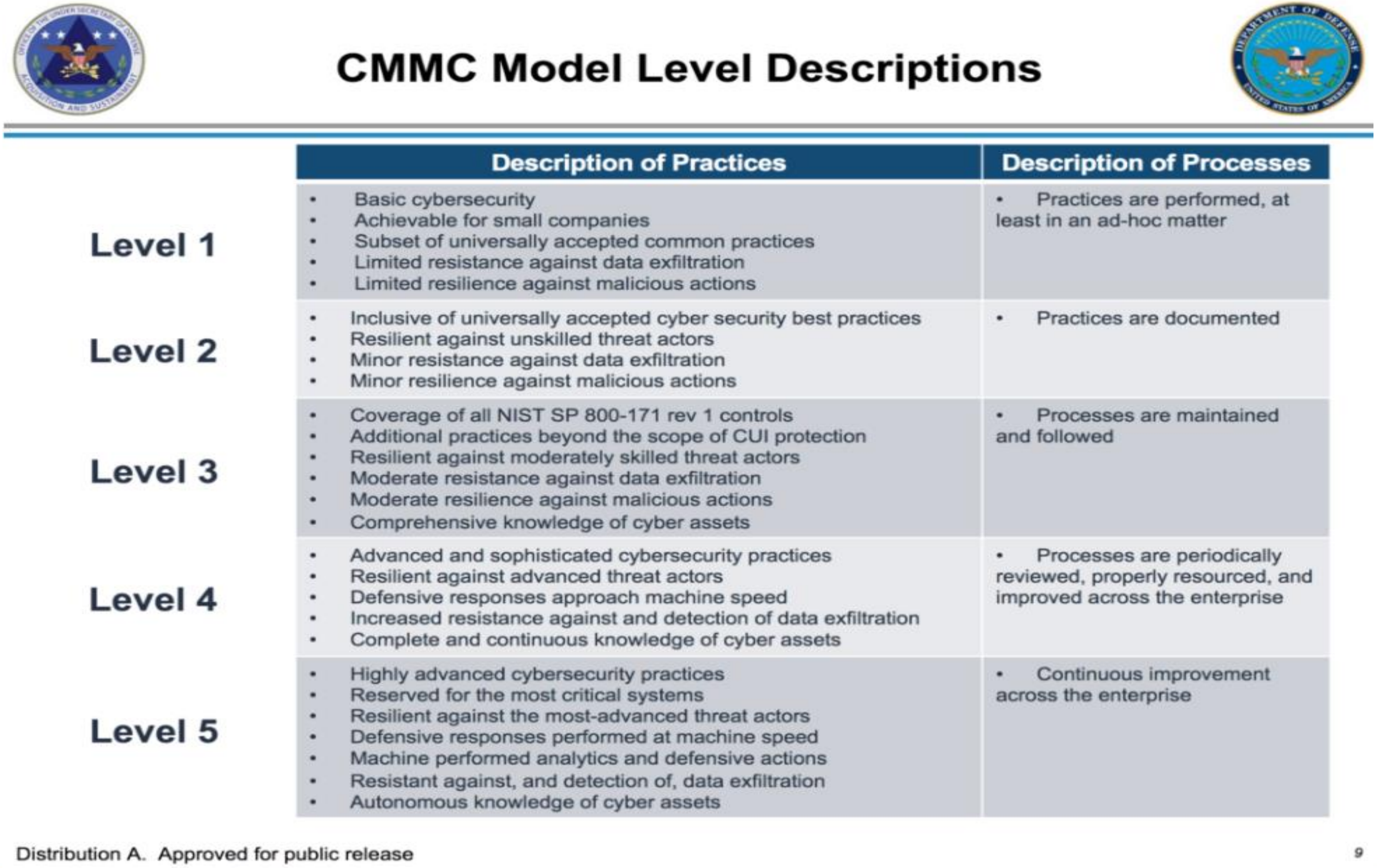
Office of the Under Secretary of Defense for
Acquisition & Sustainment
Cybersecurity Maturity Model Certification

Last updated on December 10, 2020

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) recognizes that security is foundational to acquisition and should not be traded along with cost, schedule, and performance moving forward. The Department is committed to working with the Defense Industrial Base (DIB) sector to enhance the protection of controlled unclassified information (CUI) within the supply chain.

OUSD(A&S), working with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry, developed the Cybersecurity Maturity Model Certification (CMMC) framework.

- The CMMC will review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels that range from basic cyber hygiene to advanced. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats.
- The CMMC effort builds upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements.
- The goal is for CMMC to be cost-effective and affordable for small businesses to implement at the lower CMMC levels.
- Authorized and accredited CMMC Third Party Assessment Organizations (C3PAOs) will conduct assessments and issue CMMC certificates to Defense Industrial Base (DIB) companies at the appropriate level.



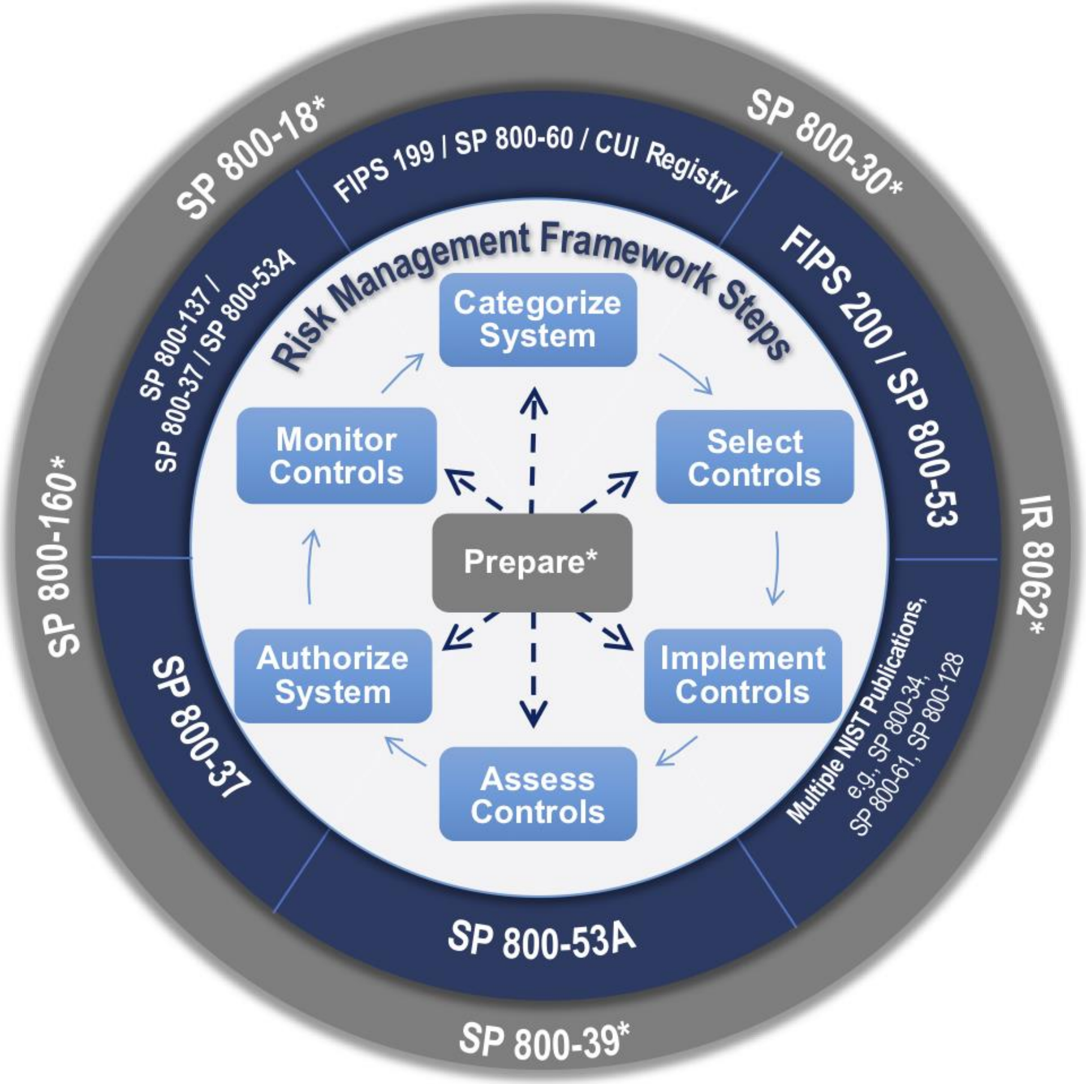
CMMC Model Level Descriptions

	Description of Practices	Description of Processes
Level 1	• Basic cybersecurity • Achievable for small companies • Subset of universally accepted common practices • Limited resistance against data exfiltration • Limited resilience against malicious actions	• Practices are performed, at least in an ad-hoc matter
Level 2	• Inclusive of universally accepted cyber security best practices • Resilient against unskilled threat actors • Minor resistance against data exfiltration • Minor resilience against malicious actions	• Practices are documented
Level 3	• Coverage of all NIST SP 800-171 rev 1 controls • Additional practices beyond the scope of CUI protection • Resilient against moderately skilled threat actors • Moderate resistance against data exfiltration • Moderate resilience against malicious actions • Comprehensive knowledge of cyber assets	• Processes are maintained and followed
Level 4	• Advanced and sophisticated cybersecurity practices • Resilient against advanced threat actors • Defensive responses approach machine speed • Increased resistance against and detection of data exfiltration • Complete and continuous knowledge of cyber assets	• Processes are periodically reviewed, properly resourced, and improved across the enterprise
Level 5	• Highly advanced cybersecurity practices • Reserved for the most critical systems • Resilient against the most-advanced threat actors • Defensive responses performed at machine speed • Machine performed analytics and defensive actions • Resistant against, and detection of, data exfiltration • Autonomous knowledge of cyber assets	• Continuous improvement across the enterprise

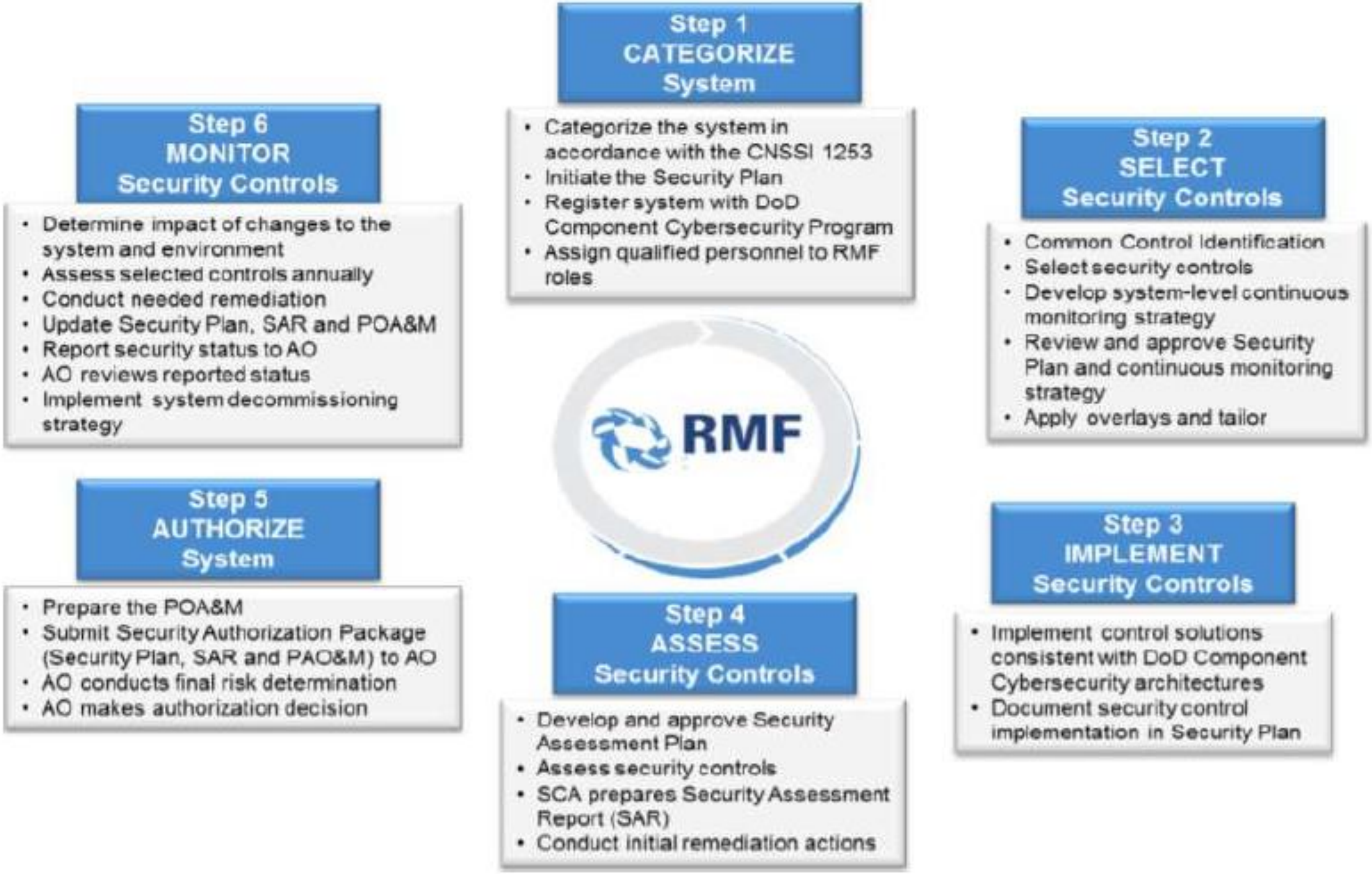
Distribution A. Approved for public release

ICS/SCADA/OT and the Risk Management Framework

- RMF is derived from NIST SP 800-53 (212 controls)
- RMF is not an easy process for ICS/SCADA/OT
- RMF is not an easy process for Legacy Systems
- RMF is not an easy process



RMF Steps



**Step 1
CATEGORIZE
System**

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

**Step 2
SELECT
Security Controls**

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

**Step 3
IMPLEMENT
Security Controls**

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

**Step 4
ASSESS
Security Controls**

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

**Step 5
AUTHORIZE
System**

- Prepare the POA&M
- Submit Security Authorization Package (Security Plan, SAR and PAO&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

**Step 6
MONITOR
Security Controls**

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

Compliance vs Intent

- Compliance does NOT equal security
- Focus should be on the intent of the standards

If you implement security from the start of the process, compliance will be a natural outcome.

Questions?

J. Brad Fuller

Director of Cyber Solutions

MartinFederal Consulting

b.fuller@martinfed.com