iFORTRISS

Cybersecurity Compliance ★ MSSP

iFORTRISS

- Woman-owned Managed Security Services Provider (MSSP)
- Cybersecurity Governance Risk & Compliance (GRC) Consulting
- **IT certified veterans** who have specific security clearances and know how to handle sensitive information
- **100% US citizen expertise in a 24/7/365 Security Operations Center (SOC)**

Heather Siemens, CEO

Brian Rhodes, CFO

iFORTRISS
Cybersecurity Compliance ★MSSP

What is the CMMC Program?

- CMMC is not new requirements; the requirements have existed for over 6.5 years.
- CMMC is a mechanism to enforce conformance with existing regulations.
- CMMC intends to ensure that those entrusted with sensitive information are capable of protecting it.

The official statement around why CMMC came about reads:

Department of Defense (DOD) is planning to migrate to the new CMC framework in order to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB). The CMMC is intended to serve as a verification mechanism to ensure appropriate levels of cybersecurity practices and processes are in place to ensure basic cyber hygiene as well as protect controlled unclassified information (CUI) that resides on the Department's industry partners' networks.

iFORTRISS
Cybersecurity Compliance ★MSSP

Why is CMMC being put into place?

- DoD and its supply chain are the targets of ongoing cyber attacks
- The consequences
  - Theft of intellectual property
  - Diminution of US military technical superiority
  - Compromise of weapon systems and platforms
- CMMC is driven by requirements of the DoD with emphasis on the DFARs (Defense Federal Acquisition Regulations)
- The primary goal of NIST 800-171 is to standardize how federal agencies define CUI (Controlled Unclassified Information)

iFORTRISS
Cybersecurity Compliance ★MSSP

History of CMMC

2017: DFARS clause 252.204-7012 introduced, requiring defense contractors to implement NIST SP 800-171 controls.

2018: DoD establishes Cybersecurity Maturity Model Certification (CMMC) program to enhance DIB cybersecurity.

2019 (January): Initial version of CMMC framework released.

2020 (September): Final version of CMMC model (v1.0) released, outlining five maturity levels.

2020 (November): CMMC 2.0 update announced, aiming to streamline certification process.

2021 (June): CMMC marketplace launched to connect assessors and organizations.

2021 (July): CMMC Level 1 (Foundational), Level 2 (Advanced), Level 3 (Expert)

Ongoing: Continuous updates and refinements to CMMC based on feedback and evolving cybersecurity landscape.

iFORTRISS
Cybersecurity Compliance ★MSSP

What's Next? (speculation)

- **2024:**
  - **CMMC Becomes Standard**: DoD makes CMMC certification mandatory for all new contracts.
  - **Better Training and Resources**: More resources allocated for contractor training and support.
  - **Pilot Programs**: Test programs launched to refine CMMC implementation.
- **2025:**
  - **Smoother Certification Process**: DoD simplifies certification process based on pilot program feedback.
  - **Continuous Monitoring**: CMMC integrated with ongoing cybersecurity monitoring.
- **2026:**
  - **Advanced Security Measures**: CMMC updated to counter new cyber threats.
  - **Broader Adoption**: CMMC expands beyond traditional defense contracts.
  - **Feedback Loop**: DoD gathers feedback for continuous improvement of CMMC program.

iFORTRISS
Cybersecurity Compliance ★MSSP

CMMC Assessment Process

- Under NIST 800-171 – any contractor today is subject to the requirements and would self attest via the Supplier Performance Risk Management (SPRS) system
- CMMC certification assessments cannot occur until DoD rulemaking is complete – tentatively estimated at Q1 of 2025
- CMMC Assessment Process (CAP) is the framework for assessment structure, workflow, etc. that will govern **C3PAO**s and the overall workflow
  - Currently in a draft state and is expected to change prior to the completion of DoD rulemaking
  - Encompasses (4) phases [planning, conduct, reporting, POA&M close-out]

iFORTRISS
Cybersecurity Compliance ★ MSSP

CMMC Compliance Elements

1. **Security Assessment Report**: Tests to find and fix security issues.
2. **Risk Assessment Report**: Identifying and managing cybersecurity risks.
3. **System Security Plan (SSP)**: Document detailing system security measures.
4. **Plans of Action and Milestones (POAM)**: Plans to fix security issues.
5. **Supplier Performance Risk System (SPRS) Score**: Rating suppliers' cybersecurity and readiness.
6. **Network Diagram**: Visual map of network setup.
7. **Controlled Unclassified Information (CUI) Flow**: Managing sensitive data movement.
8. **Asset Inventory and Categorization**: Keeping track of and organizing digital resources.

iFORTRISS
Cybersecurity Compliance ★MSSP

Definitions

- Organization Seeking Assessment (OSA): the entity seeking to conduct, obtain, or maintain a CMMC Assessment for a given information system at a particular CMMC level.
- Organization Seeking Certification (OSC): the entity seeking to conduct, obtain, or maintain a CMMC Certification for a given information system at a particular CMMC level.
- External Services Provider (ESP): external people, technology, or facilities that an organization utilizes for provision and management of comprehensive IT and or cybersecurity services on behalf of the organization. In the CMMC Program, CUl or Security Protection Data (e.g., log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP.
- Cloud Service Provider (CSP): means an external company that provides a platform, infrastructure, applications, and/or storage services for its clients
- Certified 3rd Party Assessment Organization (C3PAO): the primary role of a C3PAO is to conduct assessments on companies to ensure they meet the DoD's CMMC standards.

iFORTRISS
Cybersecurity Compliance ★MSSP

Risks and Liability

Affirmation creates potential Corporate and Personal Liability

- The **False Claims Act** provides that any person who knowingly submits, or causes to submit, false claims to the government is liable for three times the government's damages.
- The **Civil Cyber-Fraud Initiative** was launched to identify, pursue, and prosecute cybersecurity-related fraud against the government. The initiative uses the False Claims Act to hold government contractors accountable for cybersecurity and prioritizes enforcement against companies and individuals that knowingly violate cybersecurity requirements. A **"whistleblower"** provision is included that allows individuals to file suits on behalf of the United States. Whistleblowers can be awarded between 15% and 30% of damages.

iFORTRISS
Cybersecurity Compliance ★MSSP

Risks and Liability

Non-compliance affects award eligibility

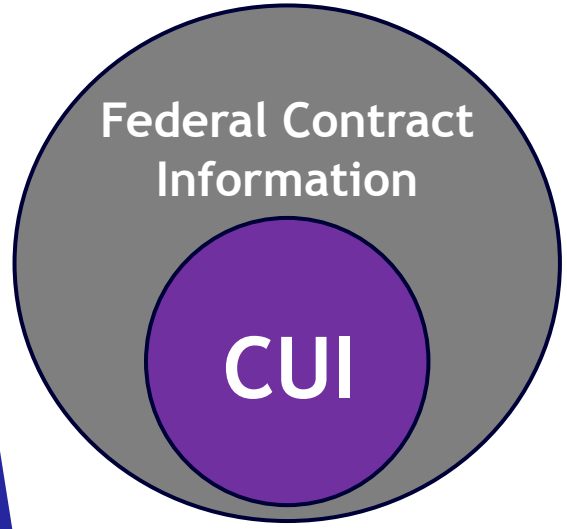
- Loss of contract (terminations for convenience/default)
- Suspension and debarment
- Lawsuits
- Investigations
- Loss of reputation
- Breach recovery costs
- False Claims Act

iFORTRISS
Cybersecurity Compliance ★MSSP

5 Basic Steps On Your Journey to CMMC Compliance

iFORTRISS
Cybersecurity Compliance ★ MSSP

1. Determine Types of Information



- Federal Contract Information (FCI)

  Information not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government

- Controlled Unclassified Information (CUI)

  Information that needs to be protected or shared according to applicable laws, regulations, and government-wide policies, but is not classified

iFORTRISS
Cybersecurity Compliance ★MSSP

2. Determine CMMC Level

I only have FCI: CMMC L1

- 17 Controls
- 59 Assessment Objectives
- Annual Self-Assessment
- Senior Official Affirmation

I have FCI & CUI: CMMC L2

- 110 Controls
- 320 Assessment Objectives
- Triennial CMMC Third Party Assessment Organization (C3PAO) Assessment
- Year 2 and 3 Annual Self-Assessment with Senior Official Affirmation

iFORTRISS
Cybersecurity Compliance ★MSSP

3. Begin Early

- Don’t wait before it’s too late.
- Plan for 12-18 Months to achieve CMMC compliance
- There are limited C3PAO Assessors <500 and 1,000’s of firms that need to be assessed.
- Expect Limited C3PAO Resources by end of 2024.

iFORTRISS
Cybersecurity Compliance ★MSSP

4. Assess Current Maturity

1. **Level 1**: Engage NIST CSF Assessor (i.e. FortifyExperts.com) – to affordably identify gaps and raise maturity. Build the foundation for remediation planning and solutioning.
2. **Level 2**: Engage CMMC Certified Assessor(i.e. iFortriss.com) for an evaluation assessment to achieve a Supplier Performance Risk System (SPRS) Score, System Security Plan (SSP), Security Assessment Report (SAR), Risk Assessment Report (RAR) and develop a Plan of Action and Milestones (POAM). This will verify your current level of readiness and prepare you for the CMMC Audit.

iFORTRISS
Cybersecurity Compliance ★MSSP

5. Outsource IT to Approved Providers

External Service Providers (ESP)	Outsourcing IT can accelerate CMMC Compliance by Offloading Scope.
Managed Security Service Providers (MSSP)	Leveraging MSSPs that offer CMMC Compliant network security services can also help organizations elevate security to a CMMC level by protecting their devices, systems, and applications from cyber threats.
Cloud Service Providers (CSP)	Identifying FedRAMP certified or equivalent on-demand cloud computing resources can simplify areas such as storage, computing power, or application security compliance.

iFORTRISS
Cybersecurity Compliance ★MSSP

You can outsource responsibility.
You cannot outsource accountability.

Questions?

For More Info:
Brian Rhodes, CFO
iFortriss.com
(214) 263-2635 Mobile
brian.rhodes@ifortriss.com

iFORTRISS
Cybersecurity Compliance ★ MSSP