govSpend

# CMMC and the New FAR: Dramatic Changes in Federal Contracting

October 21, 2025

# Agenda

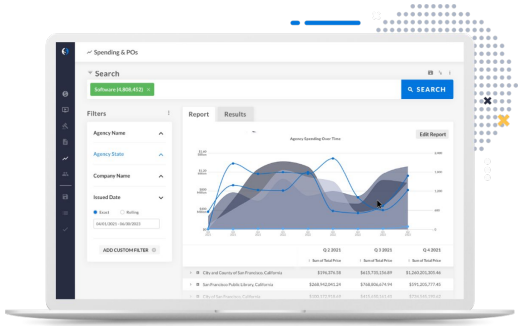
- Introduction
- Presentation by **Eric Crusius, Partner, Hunton Andrews Kurth LLP**
- Q&A

*Note: The webinar recording and presentation slides will be sent to all attendees and posted on GovSpend's website.*

govSpend

GovSpend delivers intelligence on what federal, state, and local agencies are purchasing, who they are buying from, and the precise amounts they are paying. We help you identify the specific public entities that align with your company's growth strategy, allowing you to shrewdly position yourself in the market.

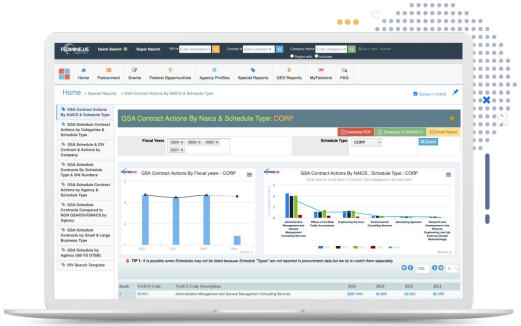
Since our acquisition of Fedmine in 2021, we're proud to be the only B2B2G companies offering both a SLED and Federal solution to our customers.




## The GovSpend Platform

**A 360° View of the SLED Market**

Unlike other public sector data providers, the GovSpend platform delivers a comprehensive view of buying and selling at the state and local levels. Whether you're looking for discussions about upcoming spending in public meetings, new Bid & RFP opportunities, or historical Agency spend down to the PO line item, you have insight into the entire lifecycle of a spending initiative.




## The Fedmine Platform

**Market Intelligence for Federal Contractors**

The Fedmine platform delivers federal contracting intelligence to government contractors and as a result, levels the playing field. By aggregating and standardizing 19 otherwise disparate data sources, Fedmine enables unparalleled access to federal spending data and gives customers robust analytics for smarter selling in the public sector.

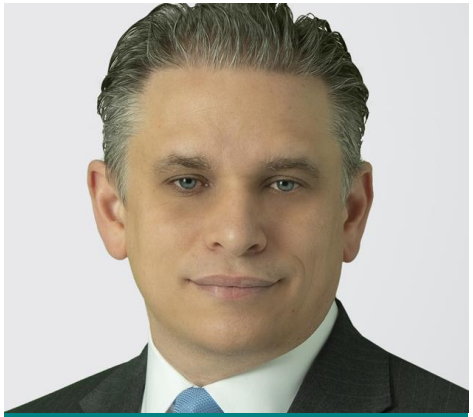
FEDCONSULT®

# Experts in Federal Procurement Data

We are a federally focused consulting firm dedicated to supporting government contractors.

With deep expertise in federal contracting and procurement data analysis, FedConsult delivers valuable insights and strategic guidance to help clients successfully navigate the complexities of the federal landscape.

# About the Presenter



**Eric S. Crusius**

Partner
Chair, Government Contracts
ecrusius@hunton.com
516.314.1307 (mobile)

Eric Crusius is a regulatory attorney based in Washington, DC, is a partner with Hunton Andrews Kurth and leads its government contracts practice.

Eric has represented clients in cybersecurity and regulatory spaces for more than 15 years and has helped some of the world's largest companies through challenges presented by selling products and services to the US federal government. This includes protests of awarded contracts in the billions of dollars, responding to cybersecurity incidents in accordance with US Department of Defense requirements, and compliance with evolving regulatory requirements.

Eric has been quoted in the Financial Times, Newsweek and in numerous industry publications. He has also appeared on NPR, Federal News Radio and Government Matters TV.

# Briefing Agenda

- Cybersecurity Initiatives
- Department of Defense (War) Initiatives
- The FAR Overhaul

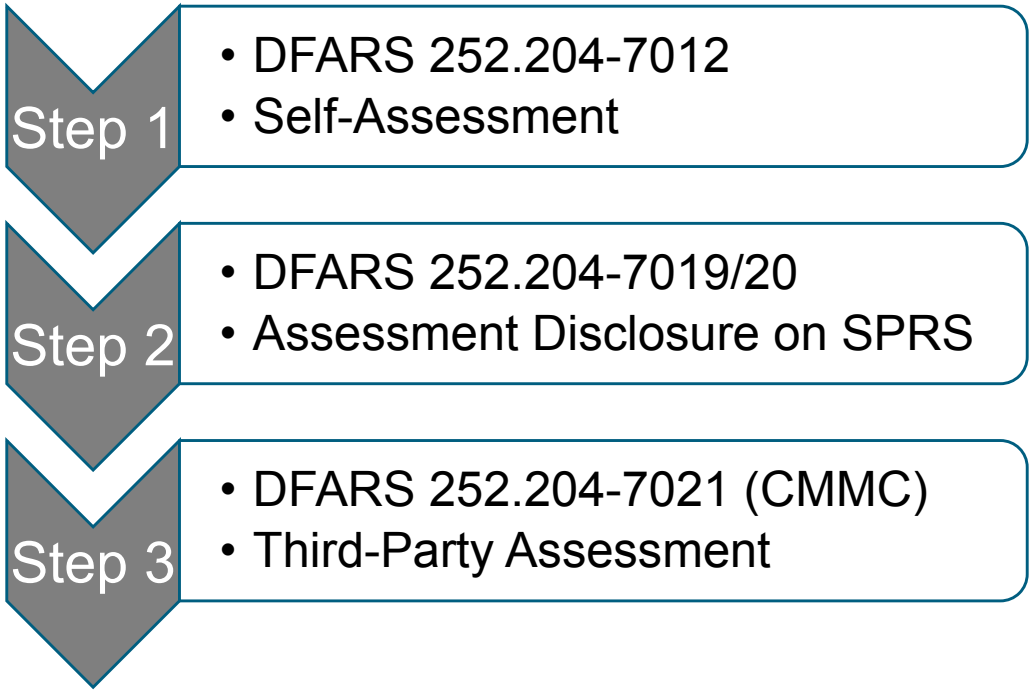
# Cybersecurity Initiatives

# Cybersecurity Initiatives – Governmentwide

- The US Government has a few governmentwide cybersecurity initiatives and some for specific agencies.
- **Governmentwide:**
  - FAR 52.204-21: 15 controls required when a company possesses Federal Contract Information (FCI). FCI is information "that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government," that is not intended for public release. Applies throughout supply chain.
  - Initiatives coming soon:
    + Compliance with 110 security controls in NIST SP 800-171 (rev 2)
    + Disclose cybersecurity incidents within 8 hours
- **The VA and DHS:**
  - New cybersecurity standards and incident disclosures. VA requires liquidated damages when certain PII is involved.

# Cybersecurity Initiatives

- US Department of Defense



# Cybersecurity Initiatives – US Dept. of Defense

**DFARS 252.204-7012 (Update Forthcoming)**

- **When it is Applicable:** when the contractor has Controlled Unclassified Information.
  - CUI is labeled by the Government OR is information of the type listed in the CUI Registry and is created or stored by the contractor in performance of the contract.

- **What it Requires:**
  - Compliance with 110 controls in NIST SP 800-171
  - Notify DOD of incidents within 72 hours
  - Cooperate with DOD in investigations
  - This clause is currently being modified by the DAR Council

- **Which revision of NIST SP 800-171?** Revision 2 (for now) under a class deviation.

# Cybersecurity Initiatives – US Dept. of Defense

**DFARS 252.204-7019/20**

- **When it is Applicable:** when the contractor has Controlled Unclassified Information.
  - CUI is labeled by the Government OR is information of the type listed in the CUI Registry and is created or stored by the contractor in performance of the contract.

- **What it Requires:**
  - Assess compliance with NIST 800-171 and provide a score in the Supplier Performance Risk System (SPRS).
  - DOD is permitted to audit scores.
  - Ensure scores are accurate and up to date.

# Cybersecurity Initiatives

PRESS RELEASE

## Defense Contractor MORSECORP Inc. Agrees to Pay $4.6 Million to Settle Cybersecurity Fraud Allegations

Wednesday, March 26, 2025

Share

**For Immediate Release**

Office of Public Affairs

MORSECORP Inc. (MORSE), of Cambridge, Massachusetts, has agreed to pay $4.6 million to resolve allegations that MORSE violated the False Claims Act by failing to comply with cybersecurity requirements in its contracts with the Departments of the Army and Air Force.

# Cybersecurity Initiatives – US Dept. of Defense

## MORSECORP ALLEGATIONS

- **Hosting Company Did Not Comply with FedRAMP:** the contractor did not ensure that the company hosting CUI met the FedRAMP Moderate baseline and complied with the Department of Defense's requirements for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis and cyber incident damage assessment.

- Lesson: use proven cloud service providers. Look on the FedRAMP marketplace. Also, ask what is their incident reporting protocol?

# Cybersecurity Initiatives – US Dept. of Defense

## MORSECORP ALLEGATIONS

- **Failure to Implement 800-171:** "the contracts required that MORSE implement all cybersecurity controls in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, but from January 2018 to February 2023, MORSE had not fully implemented all those controls…"

- Lesson: implement the NIST 800-171 controls or have POA&Ms in place.

# Cybersecurity Initiatives – US Dept. of Defense

## MORSECORP ALLEGATIONS

- **System Security Plan:** From January 2018 to January 2021, despite the contracts' system security plan requirement, MORSE did not have a consolidated written plan for each of its covered information systems describing system boundaries, system environments of operation, how security requirements are implemented and the relationships with or connections to other systems.

- Lesson: have a consolidated System Security Plan.

# Cybersecurity Initiatives – US Dept. of Defense

## MORSECORP ALLEGATIONS

- **The Wrong SPRS Score:** In January 2021, MORSE submitted a score of 104. MORSE had a third-party review done which revealed a score of -142. MORSE did not change its SPRS score until June 2023, which was three months after it was served with a subpoena.

- Lesson: have a third-party validate a SPRS score and update immediately.

# Cybersecurity Initiatives – US Dept. of Defense

- CMMC 2.0 is a new verification that contractors are complying with cybersecurity standards already in their contracts. **There are no new security controls required under CMMC.**
- The Cyber Accreditation Body is a non-profit that has a no-cost contract with the US Department of Defense and licenses assessors and other ecosystem professionals.
- For contractors with Controlled Unclassified Information, CMMC will require (in almost all cases) a third-party verification by the Certified Third-Party Assessment Organization (C3PAO).
- The Level (and security controls) required will be determined by the contracting officer.
- Contractors that have not achieved a certification in the level required will not be awarded a contract.
- While CMMC will roll out over time, it is unknown which programs will be impacted first.
- Contracts solely for the provision of COTS products will be exempt from CMMC.

# The Basics

- Third-party certifications will be handled by the Certified Third-Party Assessment Organization (C3PAO).
- The contractor defines the scope of the assessment and engages a C3PAO that has been approved by the Cyber Accreditation Body to conduct the assessment.
- The C3PAO will review each of the 110 controls and assess whether they are MET or NOT MET.
- There are three options:
  - Approval
  - Conditional approval (if 88 controls are met)
  - Not approved

# The Basics

- To determine the appropriate level, the contractor officer will determine what kind of information will be involved in the contract and assign a level?
- What is CUI?
  - 32 CFR 2002: “is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.”
  - Look to the CUI Registry: “the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.”

# The Basics

The DOD CUI Registry:

| CUI Registry Category | Examples |
|---|---|
| General Procurement and Acquisition | Contractor bid a proposal information, technical data marked proprietary, contact information for offeror |
| Source Selection | Information concerning proposed acquisitions, trade secrets, source selection information before the release of proposals |
| Controlled Technical Information | Engineering drawings, technical reports, specifications, design analysis |
| Export Controlled Information | Documents containing information controlled by ITAR/EAR, defense articles, technical data, potential/actual export control violations |
| General Proprietary Information | Trade secrets, intellectual property, confidential business information |

# Cybersecurity Initiatives – US Dept. of Defense


## Katie Arrington: Change Is Good and Change Is Coming

BY NURAY TAYLOR

APR 02, 2025

Currently performing the duties of the DoD CIO, Katie Arrington discusses upcoming changes aimed at strengthening U.S. cybersecurity.

- On CMMC: "We're waiting for the final stages, I believe, and I'm fairly certain Army's going to be the first one out of the gate with CMMC requirements."
- "The current administration is coming up with new ideas to shorten the timeframe of accomplishing critical objectives such as CMMC. And for skeptics and critics who state concerns over additional cost and expense, Arrington shared her thoughts."
- Arrington therefore noted several conversations taking place with the federal CIO about federalizing CMMC.

# Cybersecurity Initiatives – US Dept. of Defense

**Two Sets of Rules:**

- CFR Part 32–
  - Effective on December 16, 2024.
  - Establishes the entire CMMC program.
  - Rule guides certification process – certifications are happening now.

- CFR Part 48–
  - Final Rule Effective November 10, 2025.
  - Establishes clauses that go into contracts.

# Cybersecurity Initiatives – US Dept. of Defense

**CMMC Process:**

- A company that has Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) must self-assess or get a third-party assessment when clause in the contract.
- The company establishes a scope for the assessment.
- The assessment covers the system defined from the scope.
- The system assessed is given a Unique Identification Number.
- The contracting officer establishes the level needed in the solicitation and requires the assessed system UID upon award for the assessed system.

# Cybersecurity Initiatives – US Dept. of Defense

**Timing Nuances:**

- Prime contractors may require an assessment sooner than required by the Government.
- As for DOD:
  - During the first three years, the PMO will determine whether CMMC is applicable for new solicitations though this is not announced ahead of time.
  - After three years, the default is for the inclusion of CMMC.
  - Contracting officers make the decision for option years: "Contracting officers also have the discretion to bilaterally incorporate the clause in contracts awarded prior to the effective date of the clause, with appropriate consideration."

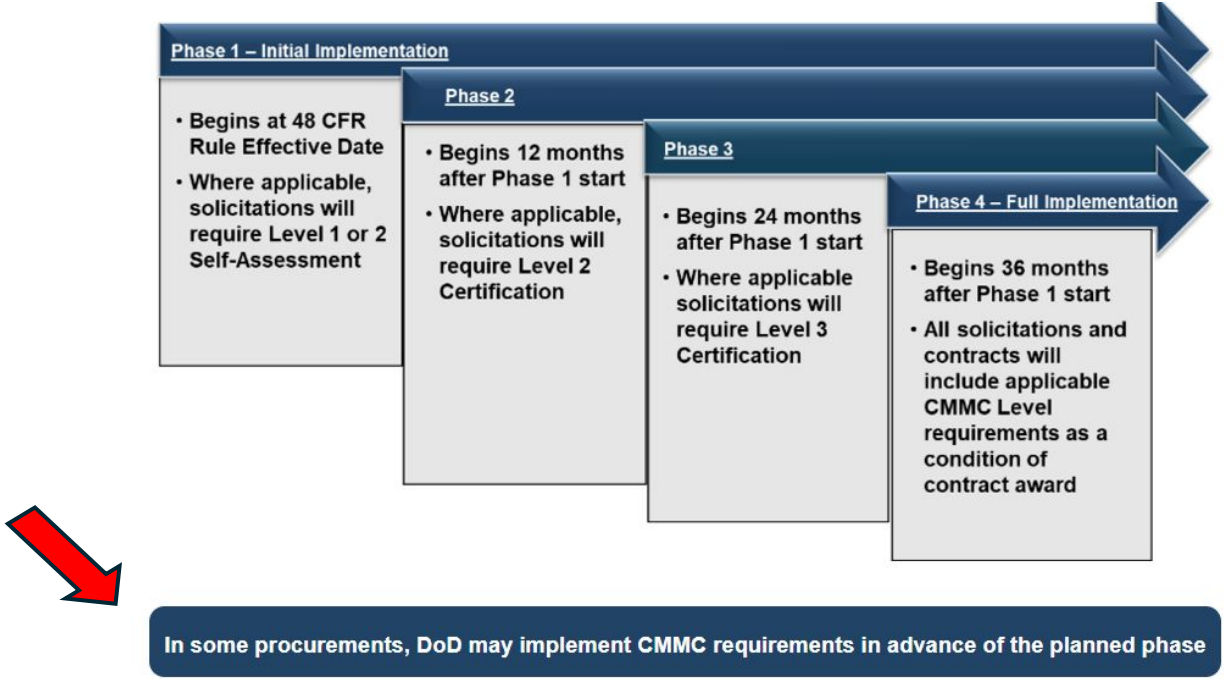
# Cybersecurity Initiatives – US Dept. of Defense

**Timing Nuances:**

- Existing contracts may be subject to CMMC sooner than new contracts
- In response to a question on existing contracts: "*DoD did not incorporate the recommendation to limit inclusion of CMMC in existing contracts unless the risk warrants inclusion, as contracting officers already have the discretion to bilaterally incorporate the clause in existing contracts based on DoD's needs. The determination to modify existing contracts after the effective date of this rule is up to the contracting officer consistent with other contractual requirements.*"

# Cybersecurity Initiatives – US Dept. of Defense

**Timing Nuances**:



# Cybersecurity Initiatives – US Dept. of Defense

- CMMC Levels 1 and 2 map to existing security requirements:

| CMMC Level | Existing Requirement | Controls | Information Type |
|---|---|---|---|
| Level 1 | FAR 52.204-21 | 15 controls in the FAR clause | Federal Contract Information |
| Level 2 | DFARS 252.204-7012 | 110 controls in NIST SP 800-171 (rev 2) | Controlled Unclassified Information |
| Level 3 | None – NEW | 24 controls is NIST SP 800-172 | Controlled Unclassified Information |

# Cybersecurity Initiatives – Rapid Rollout

| Phase | Est. Timing | Required | Optional |
|---|---|---|---|
| 1 | November 10, 2025 | • L1 and L2 Self-Assessments as condition of award. | • L1 and L2 Self-Assessment at option period for previously awarded contracts.<br>• L2 C3PAO (Conditional) Assessments as condition for award. |
| 2 | November 10, 2026 | • L2 C3PAO (Conditional) Assessments as condition of award. | • L3 DIBCAC (Conditional) Assessments as condition of award.<br>• May delay L2 C3PAO (Conditional) Assessments until option period. |
| 3 | November 10, 2027 | • L2 C3PAO (Conditional) Assessments for all option period for previously awarded contracts.<br>• L3 DIBCAC (Conditional) Assessments as condition of award. | • May delay L3 DIBCAC (Conditional) Assessments until option period. |
| 4 | November 10, 2028 | • All contracts and options will have the applicable CMMC requirements. | • None. |

# Cybersecurity Initiatives – Cert Predictions

| Level | Small | Other Than Small | Total |
|---|---|---|---|
| 1<br>Self-Assessment | 142,487 | 67,053 | 209,540 |
| 2<br>Self-Assessment | 4,596 | 2,163 | 6,759 |
| 2<br>C3PAO Assessment | 80,436 | 37,853 | 118,289 |
| 3<br>DIBCAC Assessment | 2,298 | 1,082 | 3,380 |
| **Total** | **229,818** | **108,150** | **337,968** |

# Cybersecurity Initiatives – US Dept. of Defense

**Strategies and Challenges:**

- Everything changes on the effective date – need 80% compliance.
- Foreign companies face additional uncertainty.
- Subcontractors and suppliers must comply.
- CMMC may come sooner than expected.
- New assessments may be triggered early.
- Frequent affirmations create a False Claims Act risk.
- More flexibility and risks with ESPs.
- Ensuring the correct level.

# Cybersecurity Initiatives – US Dept. of Defense

**Where to find third-party assessors:**

- Available on the Cyber AB website.
- Click o the “Marketplace” section.
- Choose “C3PAO” and make sure you filter for C3PAOs.

# Revolutionary FAR Overhaul

# FAR Re-Write

FAR Re-Write proposed in Executive Order issued by Trump administration.

Would require elimination of clauses that are not required by statute or not integral to acquisition system.

Deadline: 180 days from April 15, 2025.

PRESIDENTIAL ACTIONS

RESTORING COMMON SENSE TO FEDERAL PROCUREMENT

Executive Orders | April 15, 2025

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered:

Section 1. Purpose. The Federal Government is the largest buyer of goods and services in the world -- yet conducting business with the Federal Government is often prohibitively inefficient and costly. More than 40 years ago, the Federal Acquisition Regulation (FAR) was implemented to establish uniform procedures for acquisitions across executive departments and agencies (agencies). The "vision" of the Federal Acquisition System, codified at section 1.102 of the FAR, is to "deliver on a timely basis the best value product or service to the customer, while maintaining the public's trust and fulfilling public policy objectives[.]" but since its inception, the FAR has swelled to more than 2,000 pages of regulations, evolving into an excessive and overcomplicated regulatory framework and resulting in an onerous bureaucracy.

Federal procurement under the FAR receives consistently negative assessments regarding its efficiency. Comprehensive studies such as the 2024 Senate committee report entitled "Restoring Freedom's Forge" and the 2019 report by the Advisory Panel on Streamlining and Codifying Acquisition Regulations, created by the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114-92) and made up of experts in acquisition and procurement policy, conclude that the FAR is a barrier to, rather than a prudent vehicle for, doing business with the Federal Government. Its harmful effects permeate various items paid for by

# FAR Re-Write

- Expected Process: FAR Part will be proposed for revision and class deviations will be issued requiring change immediately until formally adopted.
- **Existing contracts will not change until modified.**
- Progress so far: Most FAR parts revised and guidance issued.
- Open questions: What, that is not statutorily, will remain? Will guidance documents create more chaos? If contracting officers receive additional flexibility, will they be properly trained?
- There may be three FAR versions at the same time.

# FAR Re-Write

- Highlights:
  - Primary changes are deletions from clauses (and entire clauses) in favor of guidance.
  - FAR Part 40 collects supply chain and information security.
  - Some topics associated with commercial contracting were moved to FAR Part 12.
  - Discussions do not have to be with all parties.  This is a change from the previous version in the FAR.
  - FAR Part 16 Re-Written to allow more flexibility.

govspend

# Thank You!

support@govspend.com | (954) 420-9900 | www.govspend.com

# Contact Us


**Archisha Mehan**

archisha@fedconsult.com

240-476-4850

**Eric Crusius**

ecrusius@hunton.com

O: 202-955-1963

M: +1 202-766-0720
or 516-314-1307

LinkedIn: EricCrusius