CMMC and Beyond: The Latest in Cybersecurity and What's to Come Under the Trump Administration

Virtual | February 5, 2025 | Eric Crusius and Chris Nagel, Partners

Holland & Knight

Introductions: Eric Crusius

Partner

Tysons, VA

703-720-8042

516-314-1307

Eric.Crusius@hklaw.com

Eric Crusius is a partner with Holland & Knight and a government contracts, cybersecurity and litigation attorney who focuses his practice on a wide range of government contract matters, including bid protests, claims and disputes, compliance issues (including cybersecurity, supply chain, domestic preference, and labor) and sub-prime issues and manages high-stakes complex commercial litigations.

Eric has appeared as a guest on Government Matters TV, NPR, and Federal News Radio and has been quoted in numerous publications including Newsweek, USA Today, the Washington Post, Washington Lawyer, the Financial Times, and the Washington Business Journal.

Twitter: @EricCrusius

Today's Speakers

Christian B. Nagel

Chris Nagel is a government contracts attorney based in Holland & Knight's Tysons, Virginia office. Mr. Nagel advises businesses on a broad range of legal issues involving their relationship with the government.

Mr. Nagel represents clients in bid protests, contract claims, suspension/debarment, False Claims Act (FCA) matters and disputes between contractors. He regularly guides corporations through compliance issues, including internal investigations and employee training.

In addition, Mr. Nagel served for 12 years on active duty and as a reservist in the U.S. Marine Corps (USMC). While on active duty, he was deployed to Afghanistan, where he adjudicated claims against the North Atlantic Treaty Organization (NATO) and the U.S. government. His previous tours include stints as a special assistant U.S. attorney for the U.S. District Court for the Eastern District of Virginia, officer-in-charge of the Quantico Legal Assistance Office and as a military prosecutor.

Christian B. Nagel
(703) 720-8088
Christian.Nagel@hklaw.com
Tysons, Virginia
Denver, Colorado

Practice

- Government Contracts
- Litigation and Dispute Resolution
- Anti-Corruption and FCPA

Education

- William & Mary Law School, J.D.
- Miami University, B.A.

Bar Admission

- Colorado
- Maryland
- Virginia

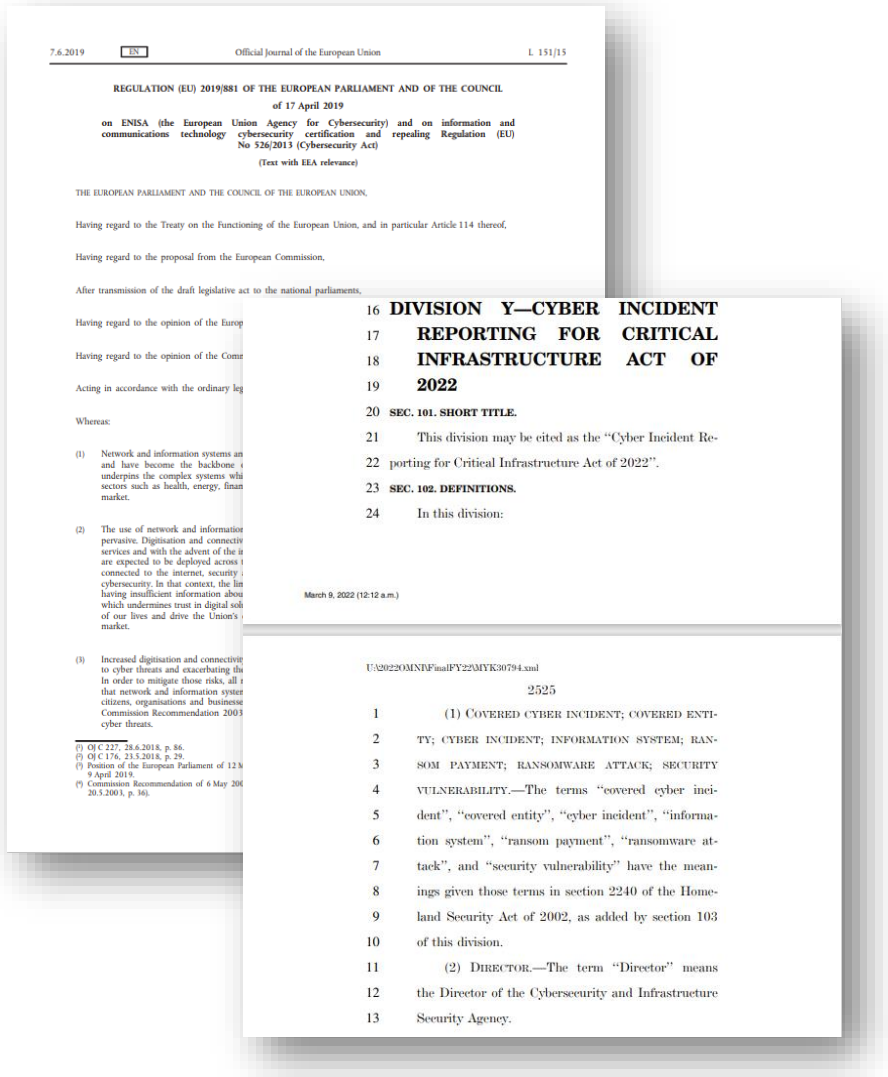
Briefing Agenda

- Introduction
- Update – New Cybersecurity Initiatives
- CMMC Program Update
- Avoiding False Claims Act Issues - Compliance Considerations

Introduction

Introduction

- The U.S. government is racing towards adoption of new cybersecurity standards.
- There are common themes:
  - Require certification of products and services (the U.S. already has the FedRAMP program for cloud service providers if U.S. government information is involved).
  - Require reporting of cybersecurity incidents within a certain time covering different sectors.



7.6.2019 EN Official Journal of the European Union L 151/15

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 17 April 2019
on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the Europ

Having regard to the opinion of the Comm

Acting in accordance with the ordinary leg

Whereas:

(1) Network and information systems ar and have become the backbone underpins the complex systems whi sectors such as health, energy, finan market.

(2) The use of network and information pervasive. Digitisation and connectiv services and with the advent of the i are expected to be deployed across connected to the internet, security cybersecurity. In that context, the lim having insufficient information abou which undermines trust in digital sol of our lives and drive the Union's market.

(3) Increased digitisation and connectivit to cyber threats and exacerbating th In order to mitigate those risks, all that network and information syster citizens, organisations and businesse Commission Recommendation 2003 cyber threats.

(1) OJ C 227, 28.6.2018, p. 86.
(2) OJ C 176, 23.5.2018, p. 29.
(3) Position of the European Parliament of 12 M 9 April 2019.
(4) Commission Recommendation of 6 May 200 20.5.2003, p. 36).

16 **DIVISION Y—CYBER INCIDENT**
17 **REPORTING FOR CRITICAL**
18 **INFRASTRUCTURE ACT OF**
19 **2022**
20 **SEC. 101. SHORT TITLE.**
21 This division may be cited as the "Cyber Incident Re-
22 porting for Critical Infrastructure Act of 2022".
23 **SEC. 102. DEFINITIONS.**
24 In this division:

March 9, 2022 (12:12 a.m.)

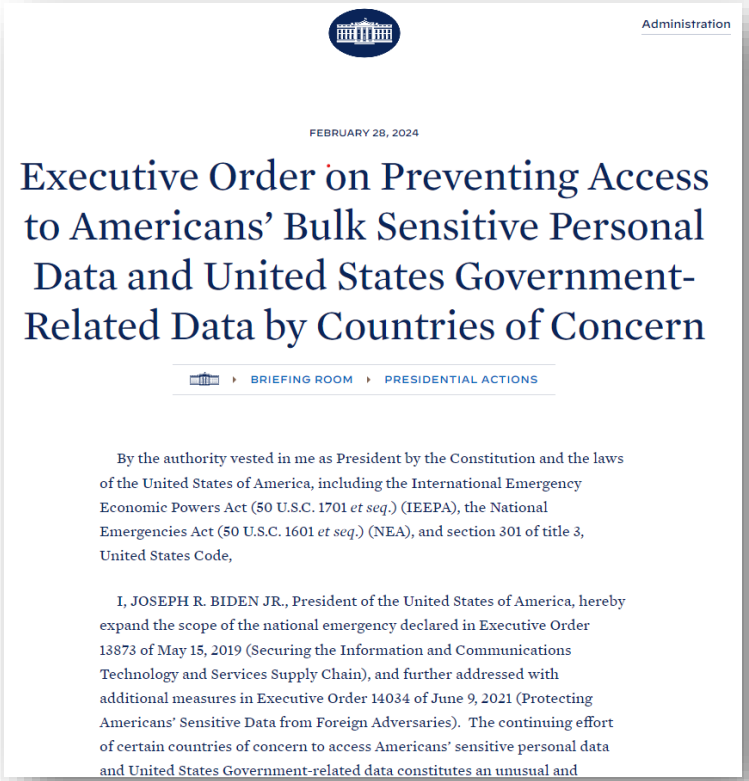
U:\2022\OMNI\FinalFY22\MYK30794.xml

2525

1 (1) COVERED CYBER INCIDENT; COVERED ENTI-
2 TY; CYBER INCIDENT; INFORMATION SYSTEM; RAN-
3 SOM PAYMENT; RANSOMWARE ATTACK; SECURITY
4 VULNERABILITY.—The terms "covered cyber inci-
5 dent", "covered entity", "cyber incident", "informa-
6 tion system", "ransom payment", "ransomware at-
7 tack", and "security vulnerability" have the mean-
8 ings given those terms in section 2240 of the Home-
9 land Security Act of 2002, as added by section 103
10 of this division.
11 (2) DIRECTOR.—The term "Director" means
12 the Director of the Cybersecurity and Infrastructure
13 Security Agency.

Introduction

- U.S. (cybersecurity) requirements can come from:
  - Local governments (local laws/regulations)
  - State governments (state laws/regulations)
  - Executive Orders issued by the President (which can become regulations)
  - Statutes passed by Congress and signed by the President (which can become regulations).
- Laws or regulations can focus on privacy, compliance or enforcing criminal compliance.



Administration

FEBRUARY 28, 2024

Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern

BRIEFING ROOM › PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), and section 301 of title 3, United States Code,

I, JOSEPH R. BIDEN JR., President of the United States of America, hereby expand the scope of the national emergency declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), and further addressed with additional measures in Executive Order 14034 of June 9, 2021 (Protecting Americans' Sensitive Data from Foreign Adversaries). The continuing effort of certain countries of concern to access Americans' sensitive personal data and United States Government-related data constitutes an unusual and

U.S. Regulatory Overview: Process

- The relevant agency will draft the regulation.
- The draft regulation is sent to the Office of Management and Budget (OMB) (specifically, the Office of Information and Regulatory Affairs, OIRA) for review.
- The regulation is approved by OIRA (or sent back to the agency) and published on the Federal Register.
- When initially published, it can be released as a proposed rule or final interim rule prior to going through the process a second time when it is a final rule.
- If proposed or final interim, members of the public will have 30-60 days to provide comments.
- The agency issuing the regulation is required to address and adjudicate each comment.

Overview of New U.S. Cybersecurity Initiatives

New Cybersecurity Initiatives

NEW FAR Cybersecurity Proposed Rule

KEY TAKEAWAY: Forthcoming requirements (governmentwide) will require incident notification requirements.

- Proposed Rule: "DoD, GSA, and NASA are proposing to amend the Federal Acquisition Regulation (FAR) to increase the sharing of information about cyber threats and incident information between the Government and certain providers, pursuant to Office of Management and Budget recommendations…"
- Requires:
  - Security incident reporting within eight hours (and follow-ups every 72 hours)
  - Definition of "incident" very broad
  - Must allow government access to compromised systems
  - Contractors must develop and maintain a software bill of materials
- Crystal ball: finalized as a rule in early 2025

New Cybersecurity Initiatives

NEW FAR Cybersecurity Proposed Rule

KEY TAKEAWAY: Forthcoming requirements (governmentwide) will require additional cybersecurity controls.

- Proposed Rule: "DoD, GSA, and NASA are proposing to amend the Federal Acquisition Regulation to standardize common cybersecurity contractual requirements across Federal agencies for unclassified Federal information systems…"
- This has been released and applies to information systems only.
- Also requires:
  - Indemnification of government for unauthorized disclosure
  - Compliance with certain security standards
- Crystal ball: final rule issued in 2025

New Cybersecurity Initiatives

NEW FAR Cybersecurity Rules

KEY TAKEAWAY: Forthcoming requirements (governmentwide) will require new cybersecurity controls.

- NIST 800-171 is coming everywhere (to the FAR Clause)
- Proposed Rule: Implements NIST 800-171 for the protection of Controlled Unclassified information (CUI) across the Government.
- Crystal ball: NPRM was released in 2024 with a final rule in 2025.

New Cybersecurity Initiatives

New CISA Cybersecurity Regulations

- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) required reporting of cybersecurity incidents.
- CISA released proposed regulations in early April.
- 72 hours to report an incident and 24 hours to report a ransomware payment.
- Critical infrastructure companies are included in requirement – definition is broad and includes wide swath of contractors.
- Some small businesses are excluded – but not defense sector small businesses or IT government contractors.
- Exclusions for “substantially similar” reporting requirements. Unknown what qualifies at this time.

New Cybersecurity Initiatives

NEW DHS Cybersecurity Readiness Factor

- Applies when contractors will have access to CUI (as defined in the regulation).
- Contractors will submit a questionnaire and will be deemed to have: (1) a high likelihood of cybersecurity readiness; (2) a likelihood of cybersecurity readiness; or (3) a low likelihood of cybersecurity readiness.
- Even with a low likelihood of cybersecurity readiness, offeror will not be eliminated though may need to take care of controls after award.
- Used in best value determinations.
- Graded against NIST SP 800-171 and SP 800-172.
- Will likely see pre-award and post-award protests about it.

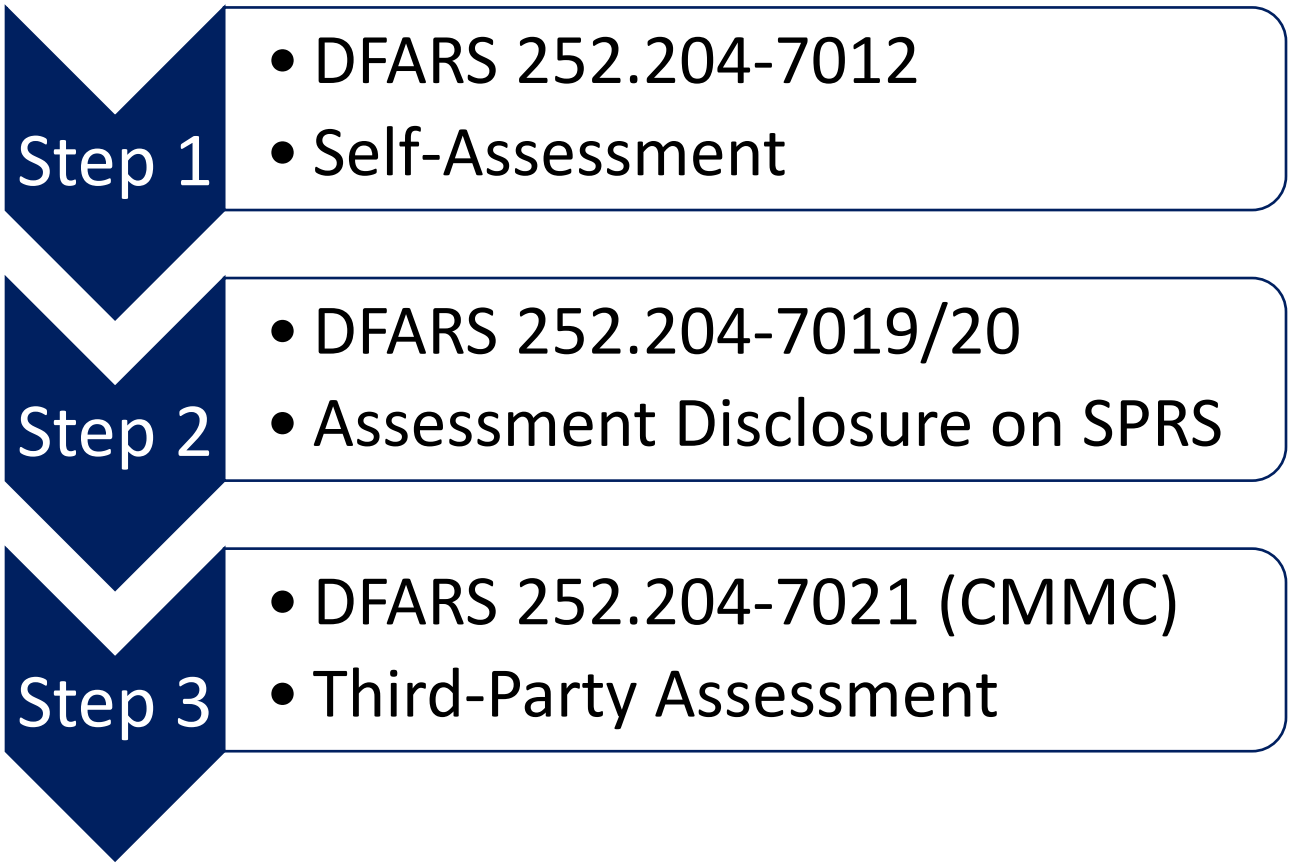
CMMC Program Update

New Cybersecurity Initiatives

- **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.

CMMC Overview

- **Department of Defense's Three Step Process**



CMMC Overview

- CMMC 2.0 is a verification that contractors are complying with cybersecurity standards already in their contracts. **There are no new security controls required under CMMC.**
- 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.

CMMC Overview

- CMMC is implemented through two sets of rules:
  - CFR Part 32:
    - The CFR Part 32 Rule describes the CMMC program and set forth the “model” or the levels and the corresponding controls.
    - The CFR Part 32 Rule is final and effective December 16, 2024.
    - Actual CMMC assessments can begin as early as the effective date.
  - CFR Part 48:
    - The CFR Part 48 Rule implements the CMMC program into contracts.
    - The proposed version of the CFR Part 48 Rule was released in August.
    - A final version of the CFR Part 48 Rule is expected to be effective in the first half of 2025.

CMMC Overview

CMMC Levels 1 and 2 Map to Current Requirements:

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

CMMC Overview

- Expected Process
  - A company that has Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) must self-assess or get a third-party assessment.
  - 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.

CMMC Overview

- The Affirmation Process – When?
  - **Level 1:** each annual self-assessment must be accompanied by an affirmation.
  - **Level 2:** affirmations must be filed:
    - At the conclusion of a third-party/self assessment
    - When POA&Ms are closed out
    - For year two and year three of a triannual assessment
  - **Level 3:** affirmations must be filed:
    - At the conclusion of a third-party assessment
    - When POA&Ms are closed out
    - For year two and year three of a triannual assessment

CMMC Overview

- The Affirmation Process – Who?
  - **Affirmation must be completed by the "Affirming Official."** The rule describes them as a "senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations." 170.22(a)(1)
- The Affirmation Process – What?
  - **Affirmation must contain the following information:** "Affirmation statement attesting that the OSA has implemented and will maintain implementation of all applicable CMMC security requirements to their CMMC Status for all information systems within the relevant CMMC Assessment Scope." 170(a)(2)(ii)

CMMC Timeline

- Original CMMC final interim rule (DFARS 252.204-21) referred to model with five levels all requiring third-party assessments.
- CMMC 2.0, announced in the Fall 2021, reduced five levels to three, eliminated DoD-specific requirements, and eliminated third-party assessments for level 1 (contractors handling federal contract information).
- On December 26, 2023, DoD released the new proposed CMMC programmatic rule and supporting documents.
- On August 15, 2024, DoD released the new proposed CMMC DFARS rule.
- In October 2024, DoD released the final programmatic rule.
- The final CMMC DFARS rule is expected Q1 2025.

CMMC Timeline

Rapid Rollout: assumes March 1, 2025 final rule effective date:

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

CMMC Impact

- DoD's certification predictions:

Level	Small	Other Than Small	Total
1 Self-Assessment	103,010	36,191	139,201
2 Self-Assessment	2,961	1,039	4,000
2 C3PAO Assessment	56,689	19,909	76,598
3 DIBCAC Assessment	1,327	160	1,487
Total	**163,987**	**57,299**	**221,286**

Avoiding the False Claims Act

CMMC Strategies and Challenges

Everything Changes on the Effective Date

- Current State: companies in the U.S. Department of Defense supply chain can have any level of compliance as long as score in SPRS is accurate.
- CMMC: 80% compliance is required (88 controls) and all outstanding controls need to be compliant within 180 days. Certain controls must be compliant on the effective date.

CMMC Strategies and Challenges

International Companies Face Uncertainty

- International companies have the same requirements as their US-based counterparts.
- As stated by DOD in response to a comment, the CMMC program "rule does not permit partial exemption of assessment requirements for foreign contractors … CMMC requirements apply to both domestic and international primes and flow down to subcontractors throughout the supply chain … regardless of where the company is headquartered or operates."
- Not all C3PAOs are willing or able to conduct assessments overseas.
- International companies may have to separate information from US-based contracts as part of its assessment scope.

CMMC Strategies and Challenges

Subcontractors and Suppliers Must Comply

- CMMC impacts subcontractors and suppliers throughout the supply chain no matter their location or status.
- The only exemption is for companies providing Commercial Off-the-Shelf (COTS) products.
- COTS products are commercial products sold in large quantities to the general public in the same form as sold to the government.
- The high-tiered contractor determines the level required based upon the information received.
- Strategies: do not share as much information or give subcontractor ability to view information (but not download it onto their system).

CMMC Strategies and Challenges

The Timeline May Accelerate

- CMMC may come sooner than expected:
  - DOD reserves the right to accelerate implementation through a bilateral modification.
  - Prime contractors may require compliance sooner.
  - It may make sense to obtain a third-party assessment instead of relying on a self-assessment from a risk perspective.

CMMC Strategies and Challenges

New Assessments May be Triggered

- New assessments are required when the scope of the system changes. This can occur with mergers and acquisition activities or system upgrades.
- If there is a lapse, the contracting officer must be notified within 72 hours and the company is not eligible for new awards or options/renewals. Also, there may be issues connected with a subcontract agreement.
- If this occurs, the legacy system should be used until the new system is able to be successfully assessed.

CMMC Strategies and Challenges

Frequent Affirmations Create a False Claims Act Risk

- A company that has received a third-party assessment or undergone a self-assessment (no matter which level) is required to file annual affirmations from an "Affirming Official." This is required for each system.
- This individual is described by DOD as someone "who is responsible for ensuring the [company's] compliance with the CMMC Program requirements and has the authority to affirm the [company's] continuing compliance with the specified security requirements for their respective organizations." 32 CFR 170.4(b).
- These affirmations are required annually for all levels of certification and are required after POA&M closeouts.

CMMC Strategies and Challenges

More Flexibility and Risks with ESPs

- External Service Providers (ESPs) providing managed services to companies are no longer required to have a Level 2 assessment (though they are in-scope and must comply with the required controls if they obtain FCI or CUI).
- More MSPs are eligible to service these companies.
- The downside is that there is no automatic good seal of approval – these companies should be thoroughly vetted to ensure they are compliant.

CMMC Strategies and Challenges

DOD is Using NIST 800-171 (Rev 2) as the Standard

- NIST 800-171 is the standard.
- NIST released Revision 3 which adds assessment goals and standards connected with supply chain requirements.
- DOD is using Revision 2 (for now) and indicated the adoption of Revision 3 would go through a rulemaking process.

CMMC Strategies and Challenges

Which Level?

- The DOD program determines the correct level.
- The level determined to be required may be artificially high or low.
- Companies have the option (if they are a prime contractor) to ask questions and/or file a bid protest prior to the time proposals are due (known as a pre-award protest).
- This will also be a point of negotiation between prime contractors and subcontractors.

CMMC Strategies and Challenges

What is Next?

- The US presidential election should not impact CMMC. The program began under the Trump administration and continued under the Biden administration.
- Implementation is expected around April 2025.
- Companies in the US defense supply chain should ensure compliance and engage with a C3PAO if they expect to hold CUI.

Compliance Considerations

Cybersecurity Compliance Considerations

Compliance Program Considerations

- **Key Risks:**
  - Requirements still amorphous; regulatory process will iron out how significant the regulations will be
  - Contractors may be obligated to report cybersecurity incidents (what to report, when to report and how to report is different across agencies)
  - Multiple certifications required
- **Compliance Program Considerations:**
  - Monitor proposed regulations and determine whether comments are advisable (or utilize a membership organization)
  - Review and update company's cybersecurity policy
  - Provide training to employees regarding cybersecurity (e.g., examples of cyber attacks, disclosure requirements, etc.)
  - Build into subcontract agreements

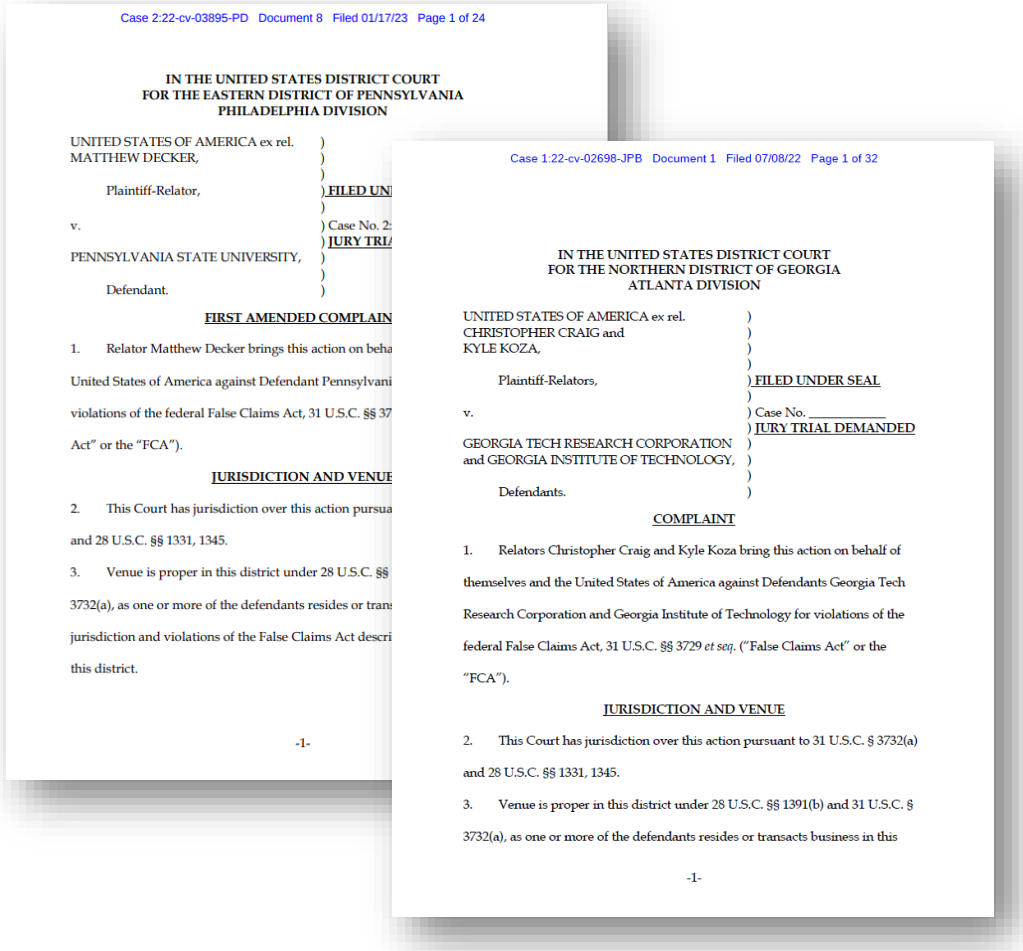
Cybersecurity Compliance Considerations

- Unknown Applicability: companies in the U.S. supply chain are required to comply even if they are far down the supply chain and do not have direct contact with the U.S. federal government.
- The Unknown Unknowns: it is difficult to know what we do not know for fast-moving developments.
- The Known Unknowns: Even known compliance requirements can create difficulties.
- Security Incidents that trigger cross-border disclosure requirements may lead to competing interests:
  - A number of U.S. regulations require companies to cooperate in cybersecurity incident investigations
  - Some U.S. regulations give U.S. government officials access to company systems.

Cybersecurity Compliance Considerations

Enforcement

- The main tool the U.S. government utilises is the False Claims Act.
- Whistleblowers also use the False Claims Act and the U.S. government has the option to intervene.



Case 2:22-cv-03895-PD Document 8 Filed 01/17/23 Page 1 of 24

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA
PHILADELPHIA DIVISION

UNITED STATES OF AMERICA ex rel.
MATTHEW DECKER,

Plaintiff-Relator,

v.

PENNSYLVANIA STATE UNIVERSITY,

Defendant.

FIRST AMENDED COMPLAIN

1. Relator Matthew Decker brings this action on beha
United States of America against Defendant Pennsylvani
violations of the federal False Claims Act, 31 U.S.C. §§ 37
Act" or the "FCA").

JURISDICTION AND VENUE

2. This Court has jurisdiction over this action pursua
and 28 U.S.C. §§ 1331, 1345.

3. Venue is proper in this district under 28 U.S.C. §§
3732(a), as one or more of the defendants resides or tran
jurisdiction and violations of the False Claims Act descri
this district.

-1-

Case 1:22-cv-02698-JPB Document 1 Filed 07/08/22 Page 1 of 32

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA ex rel.
CHRISTOPHER CRAIG and
KYLE KOZA,

Plaintiff-Relators,

v.

GEORGIA TECH RESEARCH CORPORATION
and GEORGIA INSTITUTE OF TECHNOLOGY,

Defendants.

FILED UNDER SEAL

Case No. _____

JURY TRIAL DEMANDED

COMPLAINT

1. Relators Christopher Craig and Kyle Koza bring this action on behalf of themselves and the United States of America against Defendants Georgia Tech Research Corporation and Georgia Institute of Technology for violations of the federal False Claims Act, 31 U.S.C. §§ 3729 *et seq.* ("False Claims Act" or the "FCA").

JURISDICTION AND VENUE

2. This Court has jurisdiction over this action pursuant to 31 U.S.C. § 3732(a) and 28 U.S.C. §§ 1331, 1345.

3. Venue is proper in this district under 28 U.S.C. §§ 1391(b) and 31 U.S.C. § 3732(a), as one or more of the defendants resides or transacts business in this

-1-

Further Questions

Eric Crusius
Partner
Work: +1 703-720-8042
Cell: +1 516-314-1307
Eric.Crusius@hklaw.com