Cyber Security and Beyond: The Impact of Trump Administration Policies on UK Tech Companies

From Cyber Security to Domestic Production

Eric Crusius | Partner | tech UK | 13 March 2025

HUNTON

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.

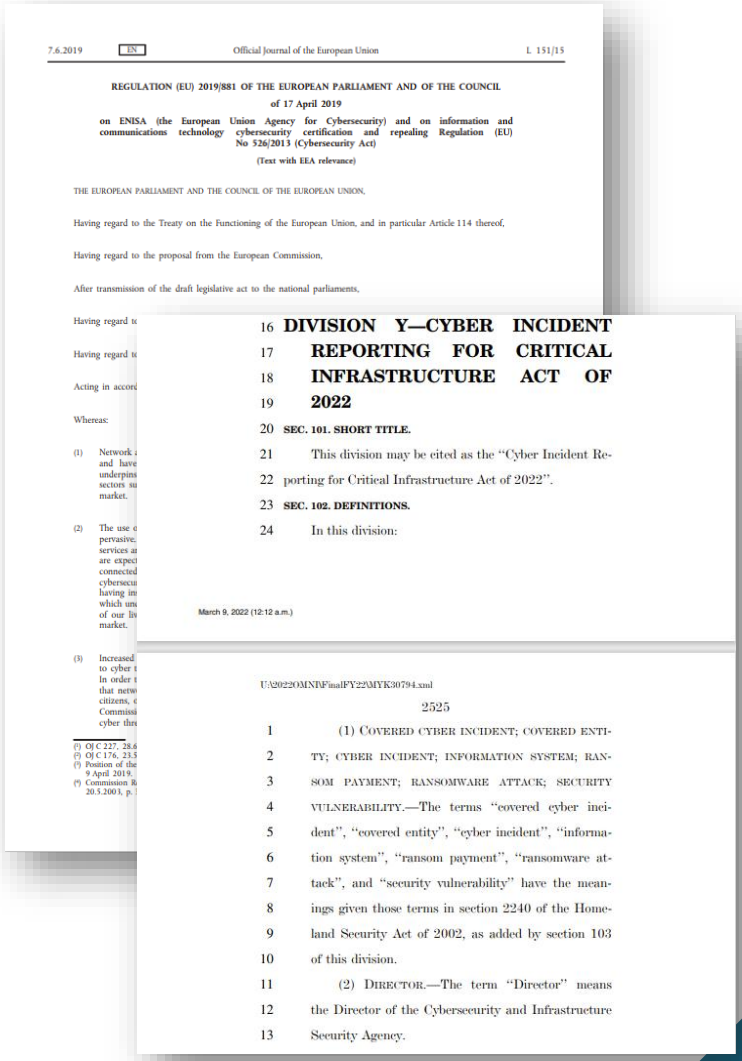
Briefing Agenda

- US Regulatory Trends
- Cyber Security Initiatives
- New Executive Orders
- Domestic Production Mandates
- Strategies for Contract Changes and Cancellations
- Looking Ahead

US Regulatory Trends

US Regulatory Trends

- 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,

DIVISION Y—CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022

SEC. 101. SHORT TITLE.

This division may be cited as the "Cyber Incident Reporting for Critical Infrastructure Act of 2022".

SEC. 102. DEFINITIONS.

In this division:

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

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

2525

(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT; INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms "covered cyber incident", "covered entity", "cyber incident", "information system", "ransom payment", "ransomware attack", and "security vulnerability" have the meanings given those terms in section 2240 of the Homeland Security Act of 2002, as added by section 103 of this division.

(2) DIRECTOR.—The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency.

HUNTON

US Regulatory Trends

- There are cyber security regulations that are industry agnostic and some that are industry specific:
  - Agnostic: new Securities and Exchange Commission (SEC) regulations aimed at requiring material cyber incident disclosures.
  - Specific:
    - Health care
    - Critical Infrastructure
    - Government contracts
- The U.S. federal government has issued 302 final regulatory actions that mention "cybersecurity" in the last year.
- The U.S. also uses a layered approach; the same company may be subject to regulations from various federal agencies in addition to state and local governments.
- For government contracts, those requirements will often be in the contracts.

US Regulatory Trends

How the US System Works

1. The relevant agency will draft the regulation.
2. The draft regulation is sent to the Office of Management and Budget (OMB) (specifically, the Office of Information and Regulatory Affairs, OIRA) for review.
3. The regulation is approved by OIRA (or sent back to the agency) and published on the Federal Register.
4. 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.
5. If proposed or final interim, members of the public will have 30-60 days to provide comments.
6. The agency issuing the regulation is required to address and adjudicate each comment.

US Regulatory Trends

- New Organization Conflict of Interest (OCI) regulations coming soon
- Existing OCI regulations (FAR 9.5) prohibit conflicts of interests with organizations selling to the US federal government
- OCI regulations generally prohibit:
  - Existence of conflicting roles that might bias the contractor's judgment
  - Unfair competitive advantage which occurs when a contractor (or prospective contractor) obtains proprietary information without proper authorization of source selection information is not available to all competitors.
- Examples:
  - Contractor that provides technical direction be awarded a contract to supply the system (or be a subcontractor in that role).
  - Contractor that provides specifications to be used in a competitive acquisition cannot be awarded a contract.

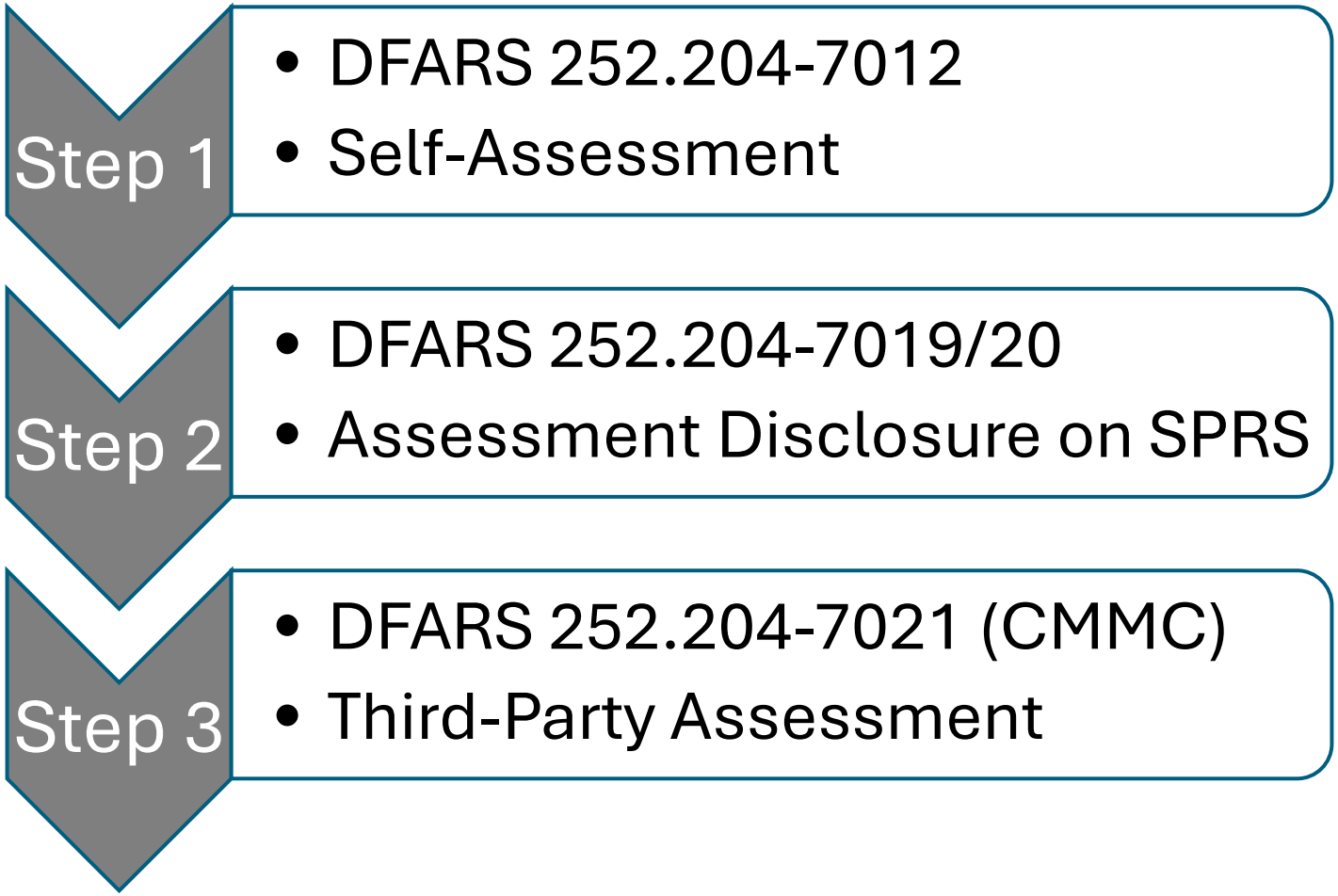
Cyber Security Initiatives

Cyber Security 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.

Cyber Security Initiatives

- US Department of Defense



Cyber Security 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.

Cyber Security 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.

Cyber Security 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-
  - Proposed rule issued August 2024.
  - Final rule expected late spring/early summer.
  - Will establish clauses that go into contracts.

Cyber Security Initiatives – US Dept. of Defense

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.

Cyber Security 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

Cyber Security Initiatives – Rapid Rollout

Phase	Est. Timing	Required	Optional
1	April 15, 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	April 15, 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	April 15, 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	April 15, 2027	• All contracts and options will have the applicable CMMC requirements.	• None.

Cyber Security Initiatives – Cert 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	56,589	19,909	76,598
3 DIBCAC Assessment	1,327	160	1,487
Total	**163,987**	**57,299**	**221,286**

Cyber Security Initiatives – US Dept. of Defense

Strategies and Challenges:

- Everything changes on the effective date – need 80% compliance.
- UK 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.

Cyber Security 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 willing to conduct assessments in the UK.

New Executive Orders

New Executive Orders

- Look for Executive Orders with immediate effect - See Executive Order 13950: "This order is effective immediately, except that the requirements of section 4 of this order shall apply to contracts entered into 60 days after the date of this order."
- Compare to EO 14055: "The Secretary of Labor (Secretary) shall, to the extent consistent with law, issue final regulations within 180 days of the date of this order to implement the requirements of this order…"
- Acceleration of Buy American policies and onshoring.
  - Government contractors versus non-government contractors.
- Overseas outsourcing prohibition and American citizenship requirements (for companies that have federal contracts).

New Executive Orders

- EOs implementing the Department of Government Efficiency.
- EO rescinding Johnson-era EO requiring affirmative action programs for federal contracts.
- New Executive Orders concerning "DEI" and related programs.
- EO rescinded a number of Biden-era executive orders:
  - Nondisplacement of Qualified Workers
  - Ethics Commitments by Executive Branch Personnel
  - Pay Transparency
  - Artificial Intelligence
- EO reinstituted a number of Trump I executive orders:
  - Requiring two regulations be repealed for every new regulation
  - Limiting use of guidance documents
  - Central repository for guidance documents

Domestic Production Mandates

Domestic Production Mandates

- DFARS 225.7004 requires the acquisition of certain components and end products manufactured within the United States, Canada, Australia, the United Kingdom, and New Zealand. They include:
  - Star trackers (navigational tools weighing more than 400 pounds in a satellite) unless Milestone A approval obtained before 1 October 2021
  - Gyrocompasses
  - Propulsion and machinery control systems
  - Propulsion system components
- The Biden administration aggressively sought to "onshore" industries that support the US federal government. It is expected that the Trump administration will continue that trend.
- Waivers are sometimes available when a domestic product is "unavailable."

Strategies for Contract Changes

Strategies for Contract Changes

- The Federal Acquisition Regulation controls what the US federal government can do when stopping or canceling an existing contract.
- While the federal government has broad termination rights, it is not unlimited and arguably a justification for each contract must be made.
- Terminated contracts are subject to termination costs submitted by the contractor that can include:
  - Lost profits
  - Material costs
  - Product costs
  - Costs for legal and accounting experts
- Depending on the vehicle, there may be limited time to seek costs.
- The Government may also issue Stop Work orders and contractors can seek increased costs (and time).

Looking Ahead

2025 and Beyond

Looking Ahead

- The US courts may act as a backstop to changes not consistent with existing law. For instance, USAID is authorized by Congress.
- Cybersecurity and domestic production requirements will continue to grow.
- Expect some contract terminations and employment separations to reverse.

Questions – Contact Information

- Phone: +1 202-955-1963
- Mobile: +1 202-766-0720
- E-Mail: ecrusius@hunton.com
- LinkedIn: EricCrusius

HUNTON